入札金額についての留意事項

1. 経費積算

経費の積算に当たっては、実施要項（案）に記載されている内容を十分理解したうえで、必要な経費を積算すること。なお、経費の費目構成については以下の通りとし、詳細な金額の内訳を経費積算表（別紙 5）に記載すること。なお、（3）印刷業務、（4）発送業務については、別紙 2 を参照の上、印刷単価表（別紙 3）、発送単価表（別紙 4）に基づき積算すること。

経費の費目構成

（1）戦略策定・企画業務
（2）応募促進業務
（3）印刷業務（単価契約）
（4）発送業務（単価契約）

※受注者に起因しない理由により、入札時から大幅な条件変更が生じた場合は、両者協議の上必要な変更を行うこととする。

2. 予算規模（税込）

上記（1）～（4）の業務すべてを実施するにあたり、以下の予算規模を上限目安として、入札金額を積算すること。

675 百万円

別紙 2

募集にかかる各種資料作成、印刷、発送業務の留意事項

1.JICA ボランティア募集関連各種資料印刷業務

1-1　業務内容

JICA ボランティア募集に関する各種資料を以下の要領で印刷する。

（1）印刷物一覧

概数は 2017 年度春募集の実績に基づいて算出した数字である。印刷部数の通知時期については、春募集分は各年 1 月末、秋募集分は各年 7 月末を予定している。

1）青年海外協力隊及び日系社会青年ボランティア（以下 JV）用募集要項セット

	内容	仕様	概数
ア	募集要項	A4 版、中綴製本、約 24 頁、4 色カラー、再生上質紙、4 色カラーコート表紙	各 18,000 部 ×8 期 （144,000 部）
イ	要請一覧	A4 版、中綴製本、約 80 頁、墨一色（うち 40 頁は 4 色カラー）、再生上質紙、4 色カラーコート表紙	
ウ	資料封入用封筒	角 2 型、4 色カラー、シール式	

2）シニア海外ボランティア及び日系社会シニア･ボランティア（以下 SV）用募集要項セット

	内容	仕様	概数
エ	募集要項	A4 版、中綴製本、約 24 頁、4 色カラー、再生上質紙、4 色カラーコート表紙	各 11,000 部 ×8 期 （88,000 部）
オ	要請一覧	A4 版、中綴製本、約 50 頁、墨一色（うち 8 頁は 4 色カラー）、再生上質紙、4 色カラーコート表紙	
カ	資料封入用封筒	角 2 型、4 色カラー、シール式	

3）JV・SV 共通資料

	内容	仕様	概数
キ	パンフレット	A4 版、中綴製本、約 30 頁、4 色カラー、マットコート表紙	29,000 部 ×8 期 （232,000 部）

4）募集要項セット用手提げビニール袋

	内容	仕様	概数
ク	手提げビニール袋（JV）	小判穴、乳白、280㎜×450㎜、両面 4 色カラー印刷、梨地、厚さ 70 ミクロン	18,000 枚 ×8 期 （144,000 枚）
ケ	手提げビニール袋（SV）	小判穴、乳白、280㎜×450㎜、両面 4 色カラー印刷、梨地、厚さ 70 ミクロン	11,000 枚 ×8 期 （88,000 枚）

ア．印刷物及び梱包資材についてはグリーン購入法基準に従うこと。なお、規格等で古紙パルプ配合率を満たさない用紙を使用せざるを得ない場合においては、オフセット等環境貢献の実施に基づく用紙を使用すること。この場合、極力古紙パルプ配合率の高い製品または森林認証など持続可能な森林経営がなされている森林から生産された原料を使用したもので、あらかじめ当機構の承認を得たものであれば可とする。納品までに、納入する用紙に関する品質証明書及びオフセット等環境貢献の実施に基づく用紙であることを確認できる書類を提出すること。

イ．印刷物のページ数については、表紙を除く本文とする。

（2）募集要項及び資料の封入

1）JV

・「ア」、「イ」及び「キ」を「ウ」へ封入する。封筒の封はせず、ベロは折る。

・資料封入後の「ウ」を「ク」へ封入する。

2）SV

・「エ」、「オ」及び「キ」を「カ」へ封入する。封筒の封はせず、ベロは折る。

・資料封入後の「カ」を「ケ」へ封入する。

（3）原稿の提供時期

１月下旬（春募集分）及び７月下旬（秋募集分）：発注者より本文原稿（一部を除く）提供

２月中旬（春募集分）及び８月中旬（秋募集分）：「オ」要請部分原稿提供

２月下旬（春募集分）及び８月下旬（秋募集分）：「イ」要請部分原稿提供

（4）留意事項
・原稿をもとに、受注者がイラストレータでレイアウト編集・加工を行う。なお、レイアウト編集に当たっては、JICA と協議の上、一般読者にとっての見やすさに配慮した構成・デザインにすること。写真は提供する。
・募集要項・要請一覧の表紙、資料封入用封筒、手提げビニール袋に関しては編集作業が発生しないものとする。デザインは提供する。
・校正は簡易校正とし、5 回程度を想定している。
・ビニール袋の校正は紙のみでの校正も可とする。（2 回程度を想定）
・校了までのスケジュールは、随時 JICA と協議のうえ進めていくこと。
・単価には、校正に関する費用も含まれる。

1-2　納品形態
（1）募集要項セット
・上記「ク」「ケ」へ封入されたものに関しては、青年とシニア毎に梱包し納品する。
・一部は手提げビニール袋（「ク」「ケ」）と資料が封入された封筒（「ウ」「カ」）を別々に納品する。

（2）印刷物の電子データ（納品先：JICA 青年海外協力隊事務局）
・印刷物 1 つにつき 1 つのファイルを PDF 形式で作成し、元データ（ai 形式）及び PDF データを 1 つの CD-R にまとめて納品する。

2. 現職教員特別参加制度関連資料印刷業務

2-1. 業務内容
　青年海外協力隊・日系社会青年ボランティア「現職教員特別参加制度」のパンフレット及び資料を以下の要領で印刷する。

(1)　印刷物一覧
　概数は 2017 年度春募集の実績に基づいて算出した数字である。印刷部数の通知時期については、各年 1 月中旬を予定している。なお、本業務は JICA ボランティアの春募集のみとし、2018 年度春募集から 2021 年度春募集までの全 4 募集期が対象となる。

	内容	仕様	概数
ア	「現職教員特別参加制度のご案内」パンフレット	A4 版、中綴製本、約 16 頁、4 色カラー、マットコート表紙両面	160,000 部×4 期（640,000 部）
イ	貼付用ポスター	A4 版、片面 4 色カラー、コート紙（110k 程度）	51,800 部×4 期(207,200 部)
ウ	送付状（計 7 種類）	A4 版、片面墨 1 色、再生上質紙	51,900 部×4 期 （207,600 部） 《一期分内訳》 ・全国教育委員会…1,800 部 ・付属学校を置く国立大学法人…60 部 ・全国国立大学法人付属学校…270 部 ・全国公立学校…39,300 部 ・各都道府県私立学校主管課…50 部 ・全国私立学校…10,350 部 ・「現職特別参加制度」参加教員…70 部
エ	送付用封筒	角２、ハイシール作成、片面印刷	51,800 部×4 期 （207,200 部）

【留意事項】

・前回原稿編集用データをもとに、イラストレータでレイアウト編集・加工を行う。なお、レイアウト編集に当たっては、JICA と協議の上、一般読者にとっての見やすさに配慮した構成・デザインにすること。
・原稿は基本的にイラストレータ、Word、Excel、PDF、PPT、idd、eps 等のデータを提供するが、一部文字データのみの場合もある。写真は提供する。
・校正は簡易校正とし、3 回程度を想定している。
・単価には、校正に関する費用も含まれる。

2-2.電子データ納品

・「ア」「イ」「エ」については、イラストレータで作成し、元データ（ai 形

式）及び PDF データを CD-R にまとめて納品する。
・「ウ」については、Word データ及び PDF データを CD-R にまとめて納品する。

2-3. 納品先
・印刷物：受注者指定発送業者、文科省及び各国内機関
・電子データ：JICA 青年海外協力隊事務局

3.JICA ボランティア募集関連各種資料発送業務
3-1　業務内容
受注者は JICA ボランティア募集関連各種資料を発送先ごとに必要な種類、数量に分別、封入、梱包し、受注者が提案した宛先へ期日までに到着するように発送する。

（1）作業コードについて
送付先の種類及び送付物の内容によって分類したコードを「作業コード」という。作業コードは、「早」、「ポＪ」、「ポG」、「ポ他」、「要Ｊ」、「両Ｊ」、「他」、「募」、「医」、「通」の全 10 種類。全送付先はコードのいずれかに分類される。作業コードごとの送付物、到着期限等については、下記「作業コード一覧表」を参照。また、作業コード毎の発送件数（2017 年度春募集の実績）は別添 12 のとおり。

【募集関連資料】作業コード一覧表

	作業ｺｰﾄﾞ	送付先	送付物				発送先への到着期限
			ポスター	募集要項セット	送付状およびFAX 送信状	医療生協用送付状・FAX 送信状	
1	**早**	制限なし	○		○		2 月および 8 月中旬
2	**ポＪ**	JICA 関係機関	○				3 月および 9 月上旬
3	**ポG**	公的機関（中央省庁・地方自治体など）	○		○		
4	**ポ他**	企業/団体/個人/その他	○		○		
5	**要Ｊ**	JICA 関係機関		○			3 月および 9 月中旬
6	**両Ｊ**	JICA 関係機関	○	○			
7	**他**	公的機関/企業/団体/個人/その他	○	○	○		

8	募	JICA 本部・JICA 国内拠点・JOCA		○			
9	医	医療生協	○			○	2 月および 8 月中旬
10	通	JICA 本部・国内拠点・JOCA	○				2 月および 8 月中旬

（2）送付物について

送付物は大きく 4 種類に分類される。受注者は作業コードごとの送付物を封入・発送すること。発注者が別途契約する印刷業者から本件受注者への送付資料の納入時期は各項目の「納入時期」に記載のとおり。

1）ポスター

ア　納入時期

・作業コード「早」「通」分：1 月および 7 月下旬

・作業コード「早」「通」以外：2 月および 8 月中旬

イ　送付物の種類　29 種（別添 2 参照）

・B1 サイズ（3 種類）

・B2 サイズ（3 種類）

・B3 サイズ（23 種類）

※ポスターの種類については変更する可能性があり、その際は速やかに通知する。

※ポスターには送付先によって、折有りタイプ、折無しタイプがある。

2）募集要項セット

ア　納入時期

・3 月および 9 月上旬

イ　送付物の種類・名称

・青年海外協力隊（約 350g）

・シニア海外ボランティア（約 300g）

※ビニール袋に角 2 封筒（中に冊子 3 冊が封入）が入ったもの、ビニール袋と封筒別のものもあり

3）送付状及び FAX 送信状

ア　納入時期

・1 月および 7 月下旬

イ　送付物の種類・名称
・送付状（A4 サイズ１枚）
・FAX 送信状（A4 サイズ１枚）

4）「医」コード用送付状及び FAX 送信状
ア　納入時期
・1 月および 7 月下旬

イ　送付物の種類・名称
・「医」コード用送付状（A4 サイズ１枚）
・FAX 送信状（A4 サイズ１枚）

（3）梱包作業について
1）梱包資材について
上記（2）の送付物を梱包する資材は全て受注者が準備すること。送付先によっては、ポスター折無しタイプ、ポスター折有りタイプ、募集要項と複数種類の送付物を送る場合があり、送付物に破損が生じないよう送付すること。また、資材についてはグリーン購入法基準に従うこと。

2）留意事項
・梱包資材表面の分かりやすい場所に、梱包されている送付物の「名称」「種類（ポスターのみ）」「部数」を明記すること。
・1 個口当たり 20kg 以下に梱包すること。
・1 件の送り先への送付物が複数口に亘る際は、各包みに〇/〇と個数を明記すること。
・異なる種類のポスターを１つの梱包資材で梱包する時は、種類ごとに別々に包装すること。
・ポスター折無しタイプは、折り目がつかないように梱包すること（丸めても良い）。折有りタイプは、すべて B5 サイズに折りたたまれている。
・送付状及び FAX 送信状は 1 番目の包みの最上部に梱包すること。
・募集要項（角 2 封筒入り）は封が開いている状態のままにしておくこと。

（4）発送作業に係る留意事項
・送付先住所一覧（発送先毎の送付内容と数量を含む）は、1 月下旬および 7 月下旬にファイルメーカーデータまたはエクセルデータで提供する。

・送付先の宛名ラベルは受注者が作成する。
・発送業務作業場所（印刷業者からの発送物の納入場所）は、関東近郊に限る。受注者が作業場所を手配すること。
・作業コードごとに指定している到着期限を厳守すること。ただし、送付物納入の遅延等、受注者の責によらない場合はその限りでない。
・発送は送付分量に合わせて経済的な発送方法（メール便、宅配便）を選択するものとする。
・宅配便「80 サイズ以下」は、3 辺（縦・横・高さ）計 80 ㎝、重量 5 ㎏までのものが対象となる。
・返送された資料については発送先情報と返送理由をリスト化し、提出すること。

3-2　作業工程表の作成について

競争参加資格確認申請時に本業務を行う場合の工程表を提出すること

3-3　発送伝票控の扱いについて

発送状況の照会を行うことがあるため、発送伝票の控えを 5 月および 11 月末日まで受注者にて保管すること。

4.現職教員特別参加制度関連資料の発送業務

4-1.業務内容

印刷業者から納入されたパンフレットを発送先ごとに必要な種類、数量に分別し、指定した発送先へ期日までに到着するように発送する。なお、本業務は JICA ボランティアの春募集のみとし、2018 年度春募集から 2021 年度春募集までの全 4 募集期が対象となる。

（1）発送先・想定発送件数

発送先は以下のとおり。想定件数は 2017 年度春募集の実績に基づく数量（閉校などにより、毎年最終的な発送件数は変更の可能性がある）。実際の発送件数は変更の可能性があり、実績に基づき精算する。

	発送先	想定件数
1	全国教育委員会（都道府県・市・特別区・町・村）：	1,788 件
2	附属学校を置く国立大学法人：	56 件

3	全国国立大学法人附属学校（幼稚園、小学校、中学校、高等学校、中等教育学校、特別支援学校）	262 件
4	全国公立学校（幼稚園、小学校、中学校、高等学校、中等教育学校、高等専門学校、特別支援学校）：	39,232 件
5	各都道府県私立学校主管課：	47 件
6	全国私立学校（幼稚園、小学校、中学校、高等学校、中等教育学校、特別支援学校）：	10,312 件
7	「現職教員特別参加制度」参加教員：	66 件
	計	51,763 件

（2）送付物について

以下 3 種の資料を封筒（角 2 サイズ、ハイシール）に封入し、封緘する（発送先 1～7 共通）。

① 送付状：1 部

送付状は、ア）各教育委員会教育長宛、（イ）附属学校を置く各国立大学法人学長宛、（ウ）各国立大学法人附属学校長宛、（エ）各公立学校長宛、（オ）各都道府県私立学校主管課長宛（カ）各私立学校長宛、（キ）「現職教員特別参加制度」参加教員宛の 7 種あるので、発送先によって（ア）～（キ）の該当する送付状を封入すること。

②現職教員特別参加制度のご案内パンフレット：3 部

③貼付用ポスター：1 部

（3） 発送作業に係る留意事項

・送付先住所一覧（発送先毎に封緘する送付状種類の指定を含む）は、各年 1 月中旬に送付する。
・発送時期は、各年 2 月中旬を予定している。
・送付先の宛名ラベルは受注者が作成する。

4-2. 発送伝票控の扱いについて

発送状況の照会を行うことがあるため、発送伝票の控えを下記の期日まで受注者にて保管すること。

2018 年度春募集：2019 年 3 月 31 日まで

2019 年度春募集：2020 年 3 月 31 日まで

別紙２

2020 年度春募集：2021 年 3 月 31 日まで
2021 年度春募集：2022 年 3 月 31 日まで

以上

従来の実施に要した経費（2016年度分）

首都圏

	単価			回数		会場借料	合計
戦略策定・企画業務	42,319	×		2募集期	+	0	84,638
	戦略策定・企画業務　合計（①）						
募集説明会	大規模	469,387	×	20	＋	7,755,663	29,030,438
	中規模	374,970	×	20			
	小規模	208,935	×	21			
	募集説明会　合計（②）						
募集説明会の広報	781,244	×		2募集期	＋	0	1,562,488
	募集説明会の広報　合計（③）						
ボランティアセミナー	52,200	×		130回	＋	0	6,786,000
	ボランティアセミナー　合計（④）						
①+②+③+④							37,463,564
消費税8%　（⑤）							2,997,083
①+②+③+④+⑤							40,460,647

大規模：目標参集者数が151名以上
中規模：目標参集者数が81～150名まで
小規模：目標参集者数が80名まで

中部

	単価			回数		会場借料	合計
戦略策定・企画業務	78,441	×		2募集期	+	0	156,882
	戦略策定・企画業務　合計（①）						
募集説明会	大規模	502,095	×	8	＋	292,165	10,278,091
	中規模	371,747	×	8			
	小規模	272,290	×	11			
	募集説明会　合計（②）						
募集説明会の広報	964,177	×		2募集期	＋	0	1,928,354
	募集説明会の広報　合計（③）						
ボランティアセミナー	138,346	×		35回	＋	8,600	4,850,710
	ボランティアセミナー　合計（④）						
①+②+③+④							17,214,037
消費税8%　（⑤）							1,377,121
①+②+③+④+⑤							18,591,158

大規模：目標参集者数が121名以上
中規模：目標参集者数が61～120名まで
小規模：目標参集者数が60名まで

関西

	単価			回数		会場借料	合計
戦略策定・企画業務	40,675	×		2募集期	+	0	81,350
	戦略策定・企画業務　合計（①）						
募集説明会	大規模	442,361	×	6	＋	4,219,932	17,199,656
	中規模	342,440	×	16			
	小規模	269,251	×	18			
	募集説明会　合計（②）						
募集説明会の広報	778,512	×		2募集期	＋	0	1,557,024
	募集説明会の広報　合計（③）						
ボランティアセミナー	76,965	×		60回	＋	0	4,617,900
	ボランティアセミナー　合計（④）						
①+②+③+④							23,455,930
消費税8%　（⑤）							1,876,472
①+②+③+④+⑤							25,332,402

大規模：目標参集者数が151名以上
中規模：目標参集者数が81～150名まで
小規模：目標参集者数が80名まで

九州

	単価			回数		会場借料	合計
戦略策定・企画業務	4,125,000	×		1.85募集期	+	0	7,631,250
	戦略策定・企画業務　合計（①）						
募集説明会	大規模	110,000	×	2	＋	697,729	2,737,673
	中規模	60,000	×	9			
	小規模	44,136	×	29			
	募集説明会　合計（②）						
募集説明会の広報	13,889	×		2募集期	＋	0	27,776
	募集説明会の広報　合計（③）						
ボランティアセミナー	7,057	×		52回	＋	1,389	368,353
	ボランティアセミナー　合計（④）						
①+②+③+④							10,765,052
消費税8%　（⑤）							861,203
①+②+③+④+⑤							11,626,255

大規模：目標参集者数が101名以上
中規模：目標参集者数が51～100名まで
小規模：目標参集者数が50名まで

従来の実施に要した経費（直営分）

機関名	募集期	人件費（※）	直接経費				合計
			広報経費	募集説明会	ボランティアセミナー	その他募集広報活動	
JICA北海道	2016春	2,556,000	2,540,730	515,230	5,780	35,460	5,653,200
	2016秋	2,556,000	2,656,800	437,260	52,780	112,330	5,815,170
JICA東北	2016春	2,556,000	2,665,000	376,720	5,100	38,880	5,641,700
	2016秋	2,556,000	2,630,000	389,100	44,180	101,180	5,720,460
JICA二本松	2016春	2,556,000	540,000	166,540	4,600	0	3,267,140
	2016秋	2,556,000	1,288,780	424,800	19,900	16,000	4,305,480
JICA駒ヶ根	2016春	2,556,000	901,627	355,942	0	0	3,813,569
	2016秋	2,556,000	854,017	441,443	18,020	0	3,869,480
JICA北陸	2016春	2,556,000	2,954,749	380,900	0	0	5,891,649
	2016秋	2,556,000	3,258,665	333,785	0	0	6,148,450
JICA中国	2016春	2,556,000	2,589,056	578,500	88,400	361,378	6,173,334
	2016秋	2,556,000	2,575,814	645,723	23,580	517,680	6,318,797
JICA四国	2016春	2,556,000	3,087,321	579,820	5,540	177,470	6,406,151
	2016秋	2,556,000	2,798,839	669,850	107,740	231,890	6,364,319
JICA沖縄	2016春	2,556,000	1,914,930	204,248	0	20,000	4,695,178
	2016秋	2,556,000	2,798,046	196,020	38,400	20,000	5,608,466
合計		40,896,000	36,054,374	6,695,881	414,020	1,632,268	85,692,543

（※）各国内機関配属の国内協力員1名分を積算

2016年度印刷・発送業務に要した経費

【印刷業務】

作成物	2016年度秋募集		2017年度春募集	
	数量	金額	数量	金額
1.募集要項・応募関連資料				
JV用	16,350	2,239,950	18,600	1,980,900
SV用	10,150	1,471,750	11,900	1,383,970
共通パンフレット	26,500	810,900	30,500	933,300
手提げビニール袋	26,500	1,186,300	30,500	1,362,212
梱包用段ボール	1,070	95,230	925	80,325
2.現職教員特別参加制度関連資料（※）				
パンフレット	0	0	159,300	2,214,270
送付状	0	0	51,820	150,278
封筒	0	0	51,800	870,240
小計		5,804,130		8,975,495
消費税等		464,330		718,040
合計		6,268,460		9,693,535
総合計		15,961,995		

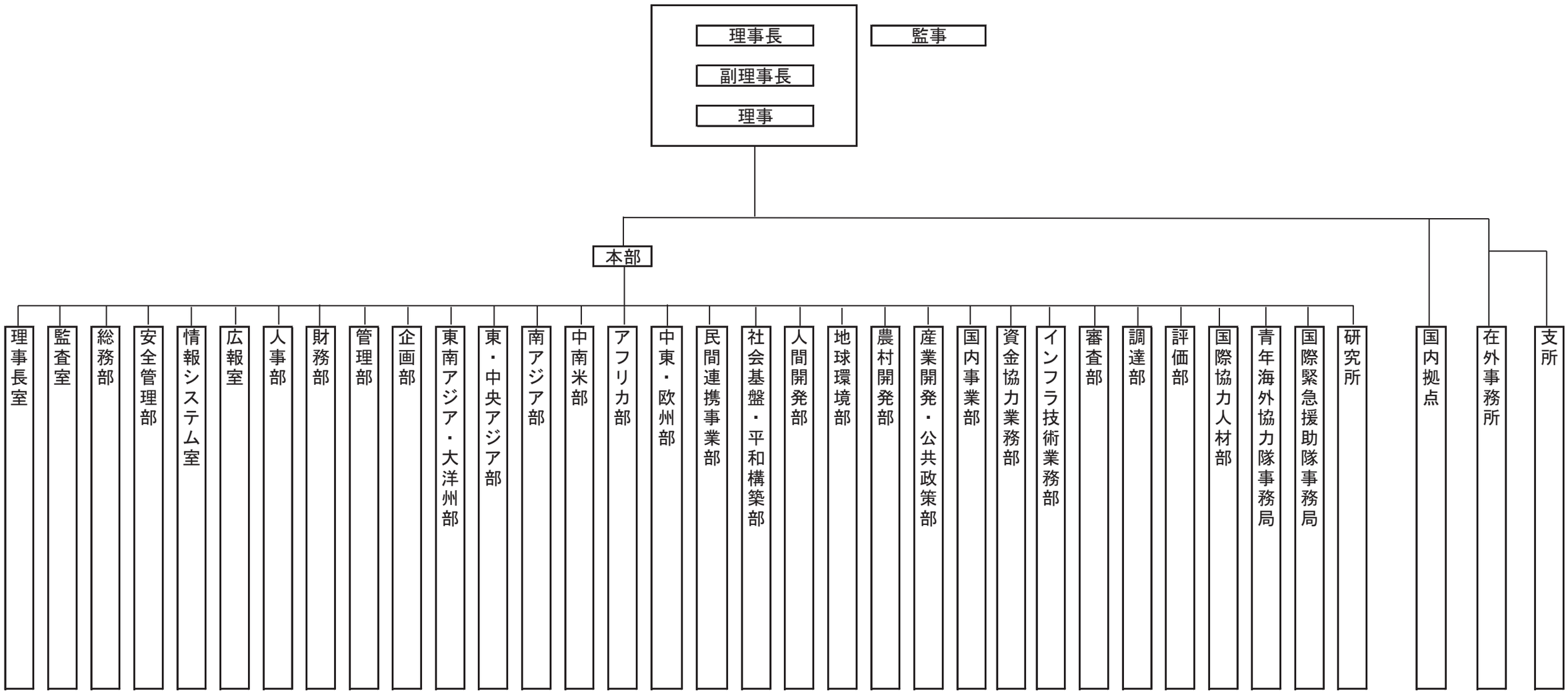
（※）現職教員特別参加制度は春募集のみ実施

【発送業務】

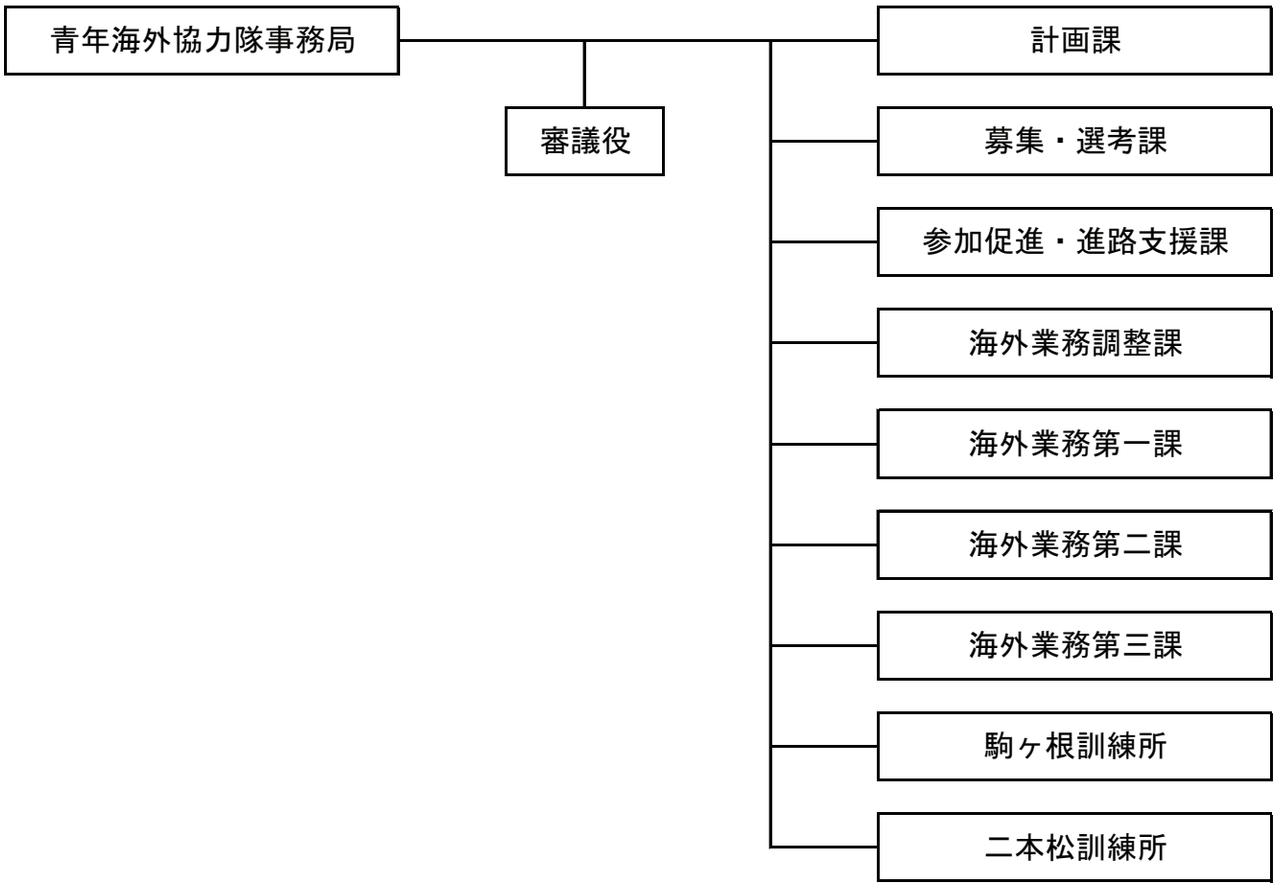
発送種別	2016年度秋募集		2017年度春募集	
	件数	金額	件数	金額
メール便	7432	542,536	7,097	518,081
宅配便（沖縄・離島）	35	111,650	40	127,600
宅配便（沖縄・離島以外）	1450	928,000	1,821	1,165,440
メール便（現職教員パンフレット）	0	0	51,763	3,360,887
小計		1,582,186		5,172,008
消費税等		126,574		413,760
合計		1,708,760		5,585,768
総合計		7,294,528		

JICA 組織図

独立行政法人国際協力機構の機構
（2017年4月1日）



青年海外協力隊事務局組織図（2017年4月1日）



国内拠点名及び所管地域

国内拠点名	所管地域
JICA北海道（札幌・帯広）	北海道
JICA東北	青森県・岩手県・宮城県・秋田県・山形県
JICA二本松	福島県
JICA筑波	茨城県・栃木県
青年海外協力隊事務局	東京都（23区）
JICA東京	群馬県・埼玉県・千葉県・東京都（23区外）・新潟県
JICA横浜	神奈川県・山梨県
JICA駒ヶ根	長野県
JICA北陸	富山県・石川県・福井県
JICA中部	岐阜県・静岡県・愛知県・三重県
JICA関西	滋賀県・京都府・大阪府・兵庫県・奈良県・和歌山県
JICA中国	鳥取県・島根県・岡山県・広島県・山口県
JICA四国	徳島県・香川県・愛媛県・高知県
JICA九州	福岡県・佐賀県・長崎県・熊本県・大分県・宮崎県・鹿児島県
JICA沖縄	沖縄県

○独立行政法人国際協力機構情報セキュリティ管理規程

(平成 29 年 4 月 3 日規程(情)第 14 号)

目次

第 1 章　目的及び適用対象(第 1 条・第 2 条)
第 2 章　情報セキュリティ対策のための基本指針(第 3 条・第 4 条)
第 3 章　情報セキュリティ対策のための基本対策(第 5 条－第 24 条)
附則

第 1 章　目的及び適用対象

(目的)

第 1 条　この規程は、政府機関等の情報セキュリティ対策の運用等に関する指針(平成 28 年 8 月 31 日サイバーセキュリティ戦略本部決定)に定める統一基準群(以下「統一基準群」という。)を踏まえ、独立行政法人国際協力機構(以下「機構」という。)がとるべき情報セキュリティの目的、対象範囲等の基本的な考え方を定めることを目的とする。

2　この規程に基づく情報セキュリティを確保するために必要な対策基準(以下「対策基準」という。)は、別に定める。

3　この規程における用語の定義は、別に定めるもののほか、次のとおりとする。

(1)　「情報システム」とは、ハードウェア及びソフトウェアからなるシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、機構が調達又は開発するもの(管理を外部委託しているシステムを含む。) をいう。

(2)　「機構情報セキュリティポリシー」(以下「機構ポリシー」という。)とは、機構の情報セキュリティ対策の基本的な方針であるこの規程及び対策基準を定める細則をいう。

(適用対象)

第 2 条　この規程の適用対象とする者は、次に掲げる者とする。

(1)　機構の役職員、非常勤勤務者及び名称の如何を問わず機構の指揮命令を受けて業務に従事する者(以下「役職員等」という。)

(2)　前項に掲げる者以外で、機構と契約上の守秘義務を負い、かつ、機構の保有する情報を取り扱う者(以下「情報取扱事務従事者」という。)

2　この規程の適用対象とする情報は、次のとおりとする。

(1)　役職員等及び情報取扱事務従事者が職務上使用することを目的として機構が調達し、又は開発した情報システム又は電磁的記録媒体に記録された情報(当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。)

(2)　その他の情報システム又は電磁的記録媒体に記録された情報(当該情報システムから

出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。)であって、役職員等及び情報取扱事務従事者が業務上取り扱う情報
(3)　(1)及び(2)のほか、機構が調達し、又は開発した情報システムの設計又は運用管理に関する情報
第 2 章　情報セキュリティ対策のための基本指針
(リスク評価と対策)
第 3 条　機構は、組織の目的等を踏まえ、自己点検結果、各種監査の結果を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講ずるものとする。
2　機構は、前項の評価に変化が生じた場合には、情報セキュリティ対策を見直すものとする。
(情報セキュリティポリシー)
第 4 条　機構は、対策基準を「政府機関の情報セキュリティ対策のための統一基準」(平成 28 年 8 月 31 日サイバーセキュリティ戦略本部決定。以下「統一基準」という。)と同等以上の情報セキュリティ対策が可能となるように定めるものとする。
2　機構は、前条第 1 項の評価の結果を踏まえ、機構ポリシーの評価及び見直しを行うものとする。
第 3 章　情報セキュリティ対策のための基本対策
(管理体制)
第 5 条　機構は、情報セキュリティ対策を実施するための組織・体制を整備するものとする。
2　機構は、最高情報セキュリティ責任者を１人置き、情報システム室担当理事をもって充てる。
3　最高情報セキュリティ責任者は、機構の情報セキュリティ対策の業務を統括するとともに、その責任を負う。
4　最高情報セキュリティ責任者は、前項に定める所管事項を対策基準に定める責任者等に分掌させることができる。
(情報セキュリティ委員会)
第 6 条　最高情報セキュリティ責任者は、機構ポリシー等の審議を行う機能を持つ組織として、機構の情報セキュリティを推進する部署及びその他業務を実施する部署の代表者を構成員とする情報セキュリティ委員会を置くものとする。
2　情報セキュリティ委員会の委員長及び委員は、最高情報セキュリティ責任者が情報セキュリティを推進する各部の代表者から指名する。委員の構成は、次のとおりとし、必要に応じ、他の役員等又は第三者の専門家を出席させることができる。
(1)　委員長 情報システム担当理事
(2)　副委員長 情報システム室長

(3)　委員 総務部長、人事部長、財務部長、管理部長及び企画部長

(対策推進計画)

第 7 条　最高情報セキュリティ責任者は、第 3 条第 1 項の評価の結果を踏まえた情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めるものとする。

[第 3 条第 1 項]

2　機構は、対策推進計画に基づき情報セキュリティ対策を実施するものとする。

3　最高情報セキュリティ責任者は、前項の実施状況を評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画の見直しを行うものとする。

(例外措置)

第 8 条　機構は、機構ポリシーに定めた情報セキュリティ対策の実施に当たり、例外措置を適用するために必要な申請・審査・承認のための手順と担当者を定める。

(教育)

第 9 条　機構は、役職員等及び情報取扱事務従事者が自覚をもって機構ポリシーに定められた情報セキュリティ対策を実施するよう、情報セキュリティに関する教育を行うものとする。

(情報セキュリティインシデントへの対応)

第 10 条　機構は、情報セキュリティインシデント(JIS Q 27000：2014 における情報セキュリティインシデントをいう。以下同じ。)に対処するため、適正な体制を構築するとともに、必要な措置を定め、実施するものとする。

2　情報セキュリティインシデント及びその可能性を認知した者は、機構ポリシーに定める報告窓口に報告するものとする。

3　機構ポリシーに定める責任者は、情報セキュリティインシデントに関して報告を受け又は認知したときは、必要な措置を講じるものとする。

(自己点検)

第 11 条　機構は、情報セキュリティ対策の自己点検を行うものとする。

(監査)

第 12 条　機構は、機構ポリシーが統一基準群に準拠し、かつ実際の運用が機構ポリシーに準拠していることを確認するため、情報セキュリティ監査を行うものとする。

(情報の格付)

第 13 条　機構は、取り扱う情報に、機密性、完全性及び可用性の観点に基づき区別し、分類した格付を付するものとする。

2　機構は、政府機関への情報の提供、運搬及び送信に際しては、前項で定めた情報の格付のうち、いかなる区分に相当するかを明示等するものとする。

(情報の取扱制限)

第 14 条　機構は、情報の格付に応じた取扱制限を定めるものとする。

2　機構は、取り扱う情報に、前項で定めたその取扱制限を付するものとする。
3　機構は、政府機関への情報の提供、運搬及び送信に際しては、情報の取扱制限を明示等するものとする。
(情報のライフサイクル管理)
第 15 条　機構は、情報の作成、入手、利用、保存、提供、運搬、送信及び消去の各段階で、情報の格付及び取扱制限に従って必要とされる取扱いが損なわれることがないように、必要な措置を定め、実施するものとする。
(情報を取り扱う区域)
第 16 条　機構は、機構が管理する事業所、又は機構外の組織から借用している施設等、機構の管理下にあり、施設及び環境に係る対策が必要な区域の範囲を定め、その特性に応じて対策を決定し、実施するものとする。
(外部委託)
第 17 条　機構は、情報処理に係る業務を外部委託する場合には、必要な措置を定め、実施するものとする。
2　機構は、外部委託を実施する場合は、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含めるものとする。
3　機構は、要機密情報を約款による外部サービスを利用して取り扱ってはならない。
4　機構は、機器等の調達に当たり、既知の脆弱性に対応していないこと、危殆化した技術を利用していること、不正プログラムを埋め込まれること等のサプライチェーン・リスクへの適切な対処を含む選定基準を整備するものとする。
(情報システムに係る文書及び台帳整備)
第 18 条　機構は、所管する情報システムに係る文書及び台帳を整備するものとする。
(情報システムのライフサイクル全般にわたる情報セキュリティの確保)
第 19 条　機構は、所管する情報システムの企画、調達・構築、運用・保守、更改・廃棄及び見直しの各段階において情報セキュリティを確保するための措置を定め、実施するものとする。
(情報システムの運用継続計画)
第 20 条　機構は、所管する情報システムに係る運用継続のための計画（以下「情報システムの運用継続計画」という。）を整備する際には、非常時における情報セキュリティ対策についても、勘案するものとする。
2　機構は、情報システムの運用継続計画の訓練等に当たっては、非常時における情報セキュリティに係る対策事項の運用が可能かどうか、確認するものとする。
(暗号・電子署名)
第 21 条　機構は、暗号及び電子署名の利用について、必要な措置を定め、実施するものとする。

（インターネット等を用いたサービスの提供）
第 22 条　機構は、インターネット等を用いて機構外にサービスを提供する際には、利用者端末の情報セキュリティ水準の低下を招く行為を防止するために、必要な措置を定め、実施するものとする。
（情報システムの利用）
第 23 条　機構は、情報システムの利用に際して、情報セキュリティを確保するために役職員等及び情報取扱事務従事者が行わなければならない必要な措置を定め、実施するものとする。
（細則等への委任）
第 24 条　この規程に定めるもののほか、この規程の実施のための手続その他の実施について必要な事項は、情報システム室長が別に定める。
附　則
この規程は、平成 29 年 4 月 3 日から施行し、平成 29 年 4 月 1 から適用する。

○情報セキュリティ管理細則

(平成 29 年 4 月 3 日細則(情)第 11 号)

目次

第 1 編　総則
　第 1 章　目的・定義・適用範囲(第 1 条－第 5 条)
　第 2 章　情報の格付の区分・取扱制限(第 6 条・第 7 条)
第 2 編　情報セキュリティ対策の基本的枠組み
　第 1 章　導入・計画(第 8 条－第 16 条)
　第 2 章　運用(第 17 条－第 25 条)
　第 3 章　点検(第 26 条－第 31 条)
　第 4 章　見直し(第 32 条・第 33 条)
第 3 編　情報の取扱い
　第 1 章　情報の取扱い(第 34 条－第 41 条)
　第 2 章　情報を取り扱う区域の管理(第 42 条－第 44 条)
第 4 編　外部委託
　第 1 章　外部委託(第 45 条－第 52 条)
第 5 編　情報システムのライフサイクル
　第 1 章　情報システムに係る文書等の整備(第 53 条－第 55 条)
　第 2 章　情報システムのライフサイクルの各段階における対策(第 56 条－第 65 条)
　第 3 章　情報システムの運用継続計画(第 66 条)
第 6 編　情報システムのセキュリティ要件
　第 1 章　情報システムのセキュリティ機能(第 67 条－第 73 条)
　第 2 章　情報セキュリティの脅威への対策(第 74 条－第 77 条)
　第 3 章　アプリケーション・コンテンツの作成・提供(第 78 条－第 82 条)
第 7 編　機構の情報システムの構成要素
　第 1 章　端末・サーバ装置等(第 83 条－第 90 条)
　第 2 章　電子メール・ウェブ等(第 91 条－第 96 条)
　第 3 章　通信回線(第 97 条－第 103 条)
第 8 編　情報システムの利用
　第 1 章　情報システムの利用(第 104 条－第 110 条)
　第 2 章　機構支給以外の端末の利用(第 111 条・第 112 条)
　附則

第 1 編　総則

第 1 章　目的・定義・適用範囲

(目的)

第 1 条　この細則は、独立行政法人国際協力機構情報セキュリティ管理規程(平成 29 年規程(情)第 14 号。以下「管理規程」という。)第 1 条第 2 項の規定に基づき、独立行政法人国際協力機構(以下「機構」という。)の情報セキュリティを確保するために必要な対策基準を定める。

(用語定義)

第 2 条　この細則における用語の定義は、管理規程に定めるもののほか次のとおりとする。

(1)　「アプリケーション・コンテンツ」とは、アプリケーションプログラム、ウェブコンテンツ等の総称をいう。

(2)　「部等」とは、組織規程第 4 条に定める本部の部、室、事務局及び研究所、組織規程第 50 条に定める国内機関、組織規程第 57 条に定める在外事務所、組織規程第 2 条第 2 項に定める支所及び出張所をいう。

[第 4 条] [第 50 条] [第 57 条]

(3)　「課等」とは、独立行政法人国際協力機構組織規程(平成 16 年規程(総)第 4 号。以下「組織規程」という。)第 6 条第 1 項及び第 6 項に定める本部の課、室及びチーム並びに組織規程第 53 条第 1 項に定める国内機関の課をいう。

[独立行政法人国際協力機構組織規程(平成 16 年規程(総)第 4 号。以下「組織規程」という。)第 6 条第 1 項] [第 6 項] [組織規程第 53 条第 1 項]

(4)　「可用性」とは、情報へのアクセスを認められたものが、必要時に中断することなく、情報にアクセスすることができる特性をいう。

(5)　「完全性」とは、情報が破壊、改ざん又は消去されていない特性をいう。

(6)　「外部委託」とは、機構の情報処理業務の一部又は全部について、「委任」「準委任」「請負」といった契約形態を問わず、契約をもって機構外の者に実施させることをいう。

(7)　「機器等」とは、情報システムの構成要素(サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等)、外部電磁的記録媒体等の総称をいう。

(8)　「機密性」とは、情報に関して、アクセスを認められた者のみが、これにアクセスできる特性をいう。

(9)　「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物(以下「書面」という。)と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの(以下「電磁的記録」という。)に係る記録媒体(以下「電磁的記録媒体」という。)がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的

記録媒体がある。
(10)　「クラウドサービス」とは、事業者によって定義されたインターフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。
(11)　「サーバ装置」とは、情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの(搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。)をいい、特に断りがない限り、機構が調達又は開発するものをいう。
(12)　「CSIRT」(シーサート)とは、機構において発生した情報セキュリティインシデントに対処するため、機構に設置された体制をいう。Computer Security Incident Response Team の略である。
(13)　「情報セキュリティ関係規程等」とは、管理規程、この細則及びこの細則に基づき情報システム室長が別に定める実施手順その他の準内部規程を総称したものをいう。
(14)　「対策推進計画」とは、管理規程第 7 条第 1 項に定めるものをいう。
[管理規程第 7 条第 1 項]
(15)　「通信回線」とは、複数の情報システム又は機器等(機構が調達等を行うもの以外のものを含む。)の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、機構の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、機構が直接管理していないものも含まれ、その種類(有線又は無線、物理回線又は仮想回線等)は問わない。
(16)　「通信回線装置」とは、通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。
(17)　「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。
(18)　「要管理対策区域」とは、機構が管理する施設等(外部の組織から借用している施設等を含む。)機構の管理下にある区域であって、取り扱う情報を保護するために、施設及び環境に係る対策が必要な区域をいう。
(適用範囲)
第 3 条　この細則の適用範囲外の情報についての管理は、独立行政法人国際協力機構法人文書管理規程(平成 16 年規程(総)第 31 号。以下「法人文書管理規程」という。)、法人文書管理細則(平成 16 年細則(総)第 21 号)の定めるところによる。
[独立行政法人国際協力機構法人文書管理規程(平成 16 年規程(総)第 31 号。以下「法人文書管理規程」という。)] [法人文書管理細則(平成 16 年細則(総)第 21 号)]

(改正)
第 4 条　情報セキュリティ水準を適切に維持していくために、情報技術の進歩に応じて、この細則を定期的に点検し、必要に応じ規定内容の追加・修正等の改正を行う。
(法令等の遵守)
第 5 条　情報及び情報システムの取扱いに関しては、機構ポリシーのほか法令等及び情報セキュリティを巡る状況に応じて策定される政府決定等を遵守する。
第 2 章　情報の格付の区分・取扱制限
(情報の格付の区分)
第 6 条　情報について、機密性、完全性及び可用性の３つの観点を区別し、この細則で用いる格付の区分の定義を示す。
2　機密性についての格付は以下のとおりとする。
(1)　機密性 3 情報とは、業務で取り扱う情報のうち、法人文書管理規程第 2 条第 11 号に定める秘密文書に相当する機密性を要する情報を含む情報とする。
[法人文書管理規程第 2 条第 11 号]
(2)　機密性 2 情報とは、業務で取り扱う情報のうち、法人文書管理規程第 2 条第 10 号に定める内部情報区分に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性 3 情報」以外の情報とする。
[法人文書管理規程第 2 条第 10 号]
(3)　機密性 1 情報とは、法人文書管理規程第 2 条第 10 号に定めるその他区分に該当すると判断される蓋然性の高い情報を含む情報とする。
[法人文書管理規程第 2 条第 10 号]
(4)　機密性 2 情報と機密性 3 情報を「要機密情報」という。
3　完全性についての格付は以下のとおりとする。
(1)　完全性 2 情報とは、業務で取り扱う情報のうち、改ざん、誤びゅう又は破損により、国民の権利を侵害され、又は業務の適切な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報とする。
(2)　完全性 1 情報とは、完全性 2 情報以外の情報とする。
(3)　完全性 2 情報を「要保全情報」という。
4　可用性についての格付は以下のとおりとする。
(1)　可用性 2 情報とは、業務で取り扱う情報のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報とする。
(2)　可用性 1 情報とは、可用性 2 情報以外の情報とする。
(3)　可用性 2 情報を「要安定情報」という。
5　要機密情報、要保全情報又は要安定情報に一つでも該当する場合は、当該情報を「要保護情報」という。

(情報の取扱制限)
第 7 条　「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを役職員等及び情報取扱事務従事者に確実に行わせるための手段をいう。
2　役職員等及び情報取扱事務従事者は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。
3　取扱制限に関する基本的な事項は、取り扱う情報に応じて、機密性、完全性及び可用性の 3 つの観点から、統括情報セキュリティ責任者が別に定める。
第 2 編　情報セキュリティ対策の基本的枠組み
第 1 章　導入・計画
(最高情報セキュリティ責任者の統括業務)
第 8 条　最高情報セキュリティ責任者は、次に掲げる業務を統括する。
(1)　情報セキュリティ対策推進のための組織・体制の整備
(2)　機構ポリシーの決定、見直し
(3)　対策推進計画の決定、見直し
(4)　情報セキュリティインシデントに対処するために必要な指示その他の措置
(5)　前各号に掲げるもののほか、情報セキュリティに関する重要事項
(情報セキュリティ委員会の機能)
第 9 条　情報セキュリティ委員会は、次に掲げる事項を審議する。
(1)　機構ポリシー
(2)　対策推進計画
(3)　前各号に掲げるもののほか、情報セキュリティに関し必要な事項
(情報セキュリティ監査責任者の設置)
第 10 条　機構は、情報セキュリティ監査に関する業務を統括する情報セキュリティ監査責任者を置き、監査室長をもって充てる。
(統括情報セキュリティ責任者・情報セキュリティ責任者等の設置)
第 11 条　最高情報セキュリティ責任者は、部等における情報セキュリティ対策に関する業務を統括する者として、情報セキュリティ責任者１人を置き、部等の長をもって充てる。ただし、研究所においては副所長をもって充てる。
2　情報セキュリティ責任者を統括し、最高情報セキュリティ責任者を補佐する者を統括情報セキュリティ責任者とし、情報システム室長をもって充てる。
3　情報セキュリティ責任者は、第 44 条第 1 項で定める区域ごとに、当該区域における情報セキュリティ対策の業務を統括する区域情報セキュリティ責任者１人を置く。
[第 44 条第 1 項]
4　情報セキュリティ責任者は、課等ごとに情報セキュリティ対策に関する業務を統括する課等情報セキュリティ責任者１人を置く

5　情報セキュリティ責任者は、所管する情報システムに対する情報セキュリティ対策に関する業務の責任者として、情報システムセキュリティ責任者を兼ねる。

(最高情報セキュリティアドバイザーの設置)

第 12 条　最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する者を最高情報セキュリティアドバイザーとして置く。

2　最高情報セキュリティアドバイザーの業務内容は、統括情報セキュリティ責任者が最高情報セキュリティ責任者と協議のうえ定める。

(情報セキュリティインシデントに備えた体制の整備)

第 13 条　最高情報セキュリティ責任者は、CSIRT を整備し、その役割を定める。

2　CSIRT は専門的な知識又は適性を有すると認められる者で構成する。そのうち、機構における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置き、情報システム室長をもって充てる。また、CSIRT 内の業務統括及び外部との連携等を行う役職員等を定める。

3　最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。

(兼務を禁止する役割)

第 14 条　役職員等及び情報取扱事務従事者は、情報セキュリティ対策の運用において、以下の役割を兼務しない。

(1)　承認又は許可(以下この項において「承認等」という。)の申請者及び当該承認等を行う者(以下この項において「承認権限者等」という。)

(2)　監査を受ける者及びその監査を実施する者

2　役職員等及び情報取扱事務従事者は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得る。

(機構ポリシーの策定)

第 15 条　最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、統一基準群に準拠した機構ポリシーを定める。

(対策推進計画の策定)

第 16 条　最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、対策推進計画を定める。対策推進計画には、機構の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた全体方針並びに次に掲げる取組の方針・重点及びその実施時期を含める。

(1)　情報セキュリティに関する教育

(2)　情報セキュリティ対策の自己点検

(3)　情報セキュリティ監査

(4)　情報システムに関する技術的な対策を推進するための取組

(5)　前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

2　前項第 3 号の情報セキュリティ監査については、最高情報セキュリティ責任者は予め情報セキュリティ監査責任者と協議する。

第 2 章　運用

(情報セキュリティ対策に関する実施手順の整備・運用)

第 17 条　統括情報セキュリティ責任者は、機構における情報セキュリティ対策に関する実施手順を整備(整備すべき者を別に定める場合を除く。)し、実施手順に関する業務を統括し、整備状況について最高情報セキュリティ責任者に報告する。

2　統括情報セキュリティ責任者は、役職員等が雇用の開始、終了若しくは人事異動する際又は情報取扱事務従事者の業務を開始若しくは終了する際に、情報セキュリティに関して必要となる事務について細目を定める規定を整備する。

3　情報セキュリティ責任者又は課等情報セキュリティ責任者は、役職員等及び情報取扱事務従事者より情報セキュリティ関係規程等に係る課題及び問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告する。

(違反への対処)

第 18 条　役職員等及び情報取扱事務従事者は、情報セキュリティ関係規程等への違反を知った場合は、情報セキュリティ責任者にその旨を報告する。

2　情報セキュリティ責任者は、情報セキュリティ関係規程等への違反の報告を受けた場合及び自らが違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、統括情報セキュリティ責任者を通じて、最高情報セキュリティ責任者に報告する。

(例外措置手続の整備)

第 19 条　最高情報セキュリティ責任者は、例外措置の適用の申請を審査する者(以下「許可権限者」という。)及び、審査手続を定める。

2　許可権限者は統括情報セキュリティ責任者とし、例外措置の適用審査記録の台帳を整備する。

(例外措置の運用)

第 20 条　役職員等及び情報取扱事務従事者は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請する。ただし、業務の遂行に緊急を要し、当該規定の趣旨を充分尊重した取扱いを行うことができる場合であって、情報セキュリティ関係規程等の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出る。

2　許可権限者は、役職員等及び情報取扱事務従事者による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定する。

3　許可権限者は、例外措置の申請状況を台帳に記録し、最高情報セキュリティ責任者に報告する。

4　統括情報セキュリティ責任者は、例外措置の申請状況を踏まえた情報セキュリティ関係規程等の追加又は見直しの検討を行い、最高情報セキュリティ責任者に報告する。

(教育体制等の整備)

第 21 条　統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備する。

(教育の実施)

第 22 条　情報セキュリティ責任者は、役職員等及び情報取扱事務従事者に対して、情報セキュリティ関係規程等に係る教育を適切に受講させる。

2　役職員等及び情報取扱事務従事者は、教育実施計画に従って、適切な時期に教育を受講する。

3　情報セキュリティ責任者は、CSIRT に属する役職員等に教育を適切に受講させる。

4　統括情報セキュリティ責任者は、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告する。

(情報セキュリティインシデントに備えた事前準備)

第 23 条　統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む機構関係者への報告手順を整備し、役職員等及び情報取扱事務従事者に周知する。

2　統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の機構外との情報共有を含む対処手順を整備する。

3　統括情報セキュリティ責任者は、情報セキュリティインシデントに備え、業務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備する。

4　統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、業務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備する。

5　統括情報セキュリティ責任者は、情報セキュリティインシデントについて機構外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を機構外の者に明示する。

6　統括情報セキュリティ責任者は、対処手順が適切に機能することを訓練等により確認する。

(情報セキュリティインシデントへの対処)

第 24 条　役職員等及び情報取扱事務従事者は、情報セキュリティインシデントの可能性を認知した場合には、機構の報告窓口(情報システム室)に報告し、指示に従う。

2　CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行う。

3　CSIRT は、情報セキュリティインシデントであると評価した場合、最高情報セキュリティ責任者に速やかに報告する。

4　CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧告を行う。
5　情報システムセキュリティ責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、情報システム室長が別途定める対処手順及び CSIRT の指示又は勧告に従って、適切に対処する。
6　情報システムセキュリティ責任者は、認知した情報セキュリティインシデントが基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には、当該運用管理規程等に従い、適切に対処する。
7　CSIRT は、機構の情報システムについて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、所管官庁に連絡する。認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行う。
8　CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、必要に応じて対処全般に関する指示、勧告又は助言を行う。
9　CSIRT は、情報セキュリティインシデントに関する対処の内容を記録する。
（情報セキュリティインシデントの再発防止・教訓の共有）
第 25 条　情報セキュリティ責任者は、CSIRT から応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として最高情報セキュリティ責任者に報告する。
2　最高情報セキュリティ責任者は、情報セキュリティ責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示する。
3　CSIRT 責任者は、情報セキュリティインシデント対処の結果から得られた教訓を、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に共有する。
第 3 章　点検
（情報セキュリティ対策の自己点検計画の策定・手順の準備）
第 26 条　統括情報セキュリティ責任者は、対策推進計画に基づき年度自己点検計画を策定する。
2　情報セキュリティ責任者は、役職員等及び情報取扱事務従事者ごとの自己点検票及び自己点検の実施手順を整備する。
（情報セキュリティ対策の自己点検の実施）
第 27 条　情報セキュリティ責任者は、年度自己点検計画に基づき、役職員等及び情報取扱事務従事者に自己点検の実施を指示する。
2　役職員等及び情報取扱事務従事者は、情報セキュリティ責任者から指示された自己点検

票及び自己点検の手順を用いて自己点検を実施する。
(情報セキュリティ対策の自己点検結果の評価・改善)
第 28 条　統括情報セキュリティ責任者及び情報セキュリティ責任者は、役職員等及び情報取扱事務従事者による自己点検結果を分析し、評価する。統括情報セキュリティ責任者は評価結果を最高情報セキュリティ責任者に報告する。
2　最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、統括情報セキュリティ責任者及び情報セキュリティ責任者に改善を指示し、改善結果の報告を受ける。
(情報セキュリティ監査実施計画の策定)
第 29 条　情報セキュリティ監査責任者は､対策推進計画を参酌して監査実施計画を定める。
2　最高情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施の必要があると認める場合には、情報セキュリティ監査責任者に、追加の監査実施を求めることができる。
(情報セキュリティ監査の実施)
第 30 条　情報セキュリティ監査責任者は、監査実施計画に基づき、以下の事項を含む監査の実施を監査実施者に指示し、結果を監査報告書として最高情報セキュリティ責任者に報告する。
(1)　機構ポリシーに統一基準群を満たすための適切な事項が定められていること
(2)　実施手順が機構ポリシーに準拠していること
(3)　自己点検の適正性の確認を行うなどにより、被監査部門における実際の運用が情報セキュリティ関係規程等に準拠していること
(情報セキュリティ監査結果に応じた対処)
第 31 条　最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を情報セキュリティ責任者に指示する。
2　情報セキュリティ責任者は、監査報告書等に基づいて最高情報セキュリティ責任者から改善を指示されたことについて、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告する。
第 4 章　見直し
(情報セキュリティ関係規程等の見直し)
第 32 条　最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、機構ポリシーについて必要な見直しを行う。
2　統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて情報セキュリティ対策に関する実施手順を見直し、又は整備した者に対して規程の見直しを指示し、見直し結果について最高情報セキュリティ責任者に報告する。
(対策推進計画の見直し)

第 33 条　最高情報セキュリティ責任者は、情報セキュリティ対策の運用及び点検・監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策推進計画について定期的な見直しを行う。

第 3 編　情報の取扱い

第 1 章　情報の取扱い

(情報の取扱いに係る規定の整備)

第 34 条　統括情報セキュリティ責任者は、次の内容を含む情報の取扱いに関する規定を整備し、役職員等及び情報取扱事務従事者へ周知する。

(1)　情報の格付及び取扱制限についての定義

(2)　情報の格付及び取扱制限の明示等についての手続

(3)　情報の格付及び取扱制限の継承、見直しに関する手続

(利用者の責任)

第 35 条　役職員等及び情報取扱事務従事者は、自らが担当している業務の遂行のために必要な範囲に限って、情報を利用等する。

(情報の格付及び取扱制限の決定・明示等)

第 36 条　役職員等及び情報取扱事務従事者は、情報の作成時及び機構外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等する。

2　役職員等及び情報取扱事務従事者は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承する。

3　役職員等及び情報取扱事務従事者は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者(決定を引き継いだ者を含む。)又は決定者の上司(以下この章において「決定者等」という。)に確認し、その結果に基づき見直す

(情報の利用・保存)

第 37 条　役職員等及び情報取扱事務従事者は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱う。

2　役職員等及び情報取扱事務従事者は、機密性 3 情報について要管理対策区域外で情報処理を行う場合は、情報システムセキュリティ責任者の許可を得る。

3　役職員等及び情報取扱事務従事者は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずる。

4　役職員等及び情報取扱事務従事者は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理する。

5　役職員等及び情報取扱事務従事者は、USB メモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従う。

(情報の提供・公表)
第 38 条　役職員等及び情報取扱事務従事者は、情報を公表する場合には、当該情報が機密性 1 情報に格付されるものであることを確認する。
2　役職員等及び情報取扱事務従事者は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うと共に、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずる。
3　役職員等及び情報取扱事務従事者は、電磁的記録を提供又は公表する場合には、当該電磁的記録からの不用意な情報漏えいを防止するための措置を講ずる。
(情報の運搬・送信)
第 39 条　役職員等及び情報取扱事務従事者は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずる。ただし、サイバーセキュリティ基本法第 13 条に定める統一的な基準と同等以上の情報セキュリティ対策を実施している国の行政機関、独立行政法人及び特殊法人の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。
[サイバーセキュリティ基本法第 13 条]
2　役職員等及び情報取扱事務従事者は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずる。
(情報の消去)
第 40 条　役職員等及び情報取扱事務従事者は、電磁的記録媒体に保存された情報が業務上不要となった場合は、速やかに情報を消去する。
2　役職員等及び情報取扱事務従事者は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消する。
3　役職員等及び情報取扱事務従事者は、要機密情報である書面を廃棄する場合には、復元が困難な状態にする。
(情報のバックアップ)
第 41 条　役職員等及び情報取扱事務従事者は、情報の格付に応じて、適切な方法で情報のバックアップを実施する。
2　役職員等及び情報取扱事務従事者は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理する。
3　役職員等及び情報取扱事務従事者は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄する。
第 2 章　情報を取り扱う区域の管理

(要管理対策区域における対策の基準の決定)
第 42 条　統括情報セキュリティ責任者は、要管理対策区域の範囲を定める。
(1)　レベル 1 役職員等及び第三者がアクセス可能な領域
(2)　レベル 2 役職員等及び役職員等から許可された者がアクセス可能な領域
(3)　レベル 3 役職員等及び当該領域を契約上の就業場所とし所管する情報セキュリティ責任者に許可された者がアクセス可能な領域
(4)　レベル 4 役職員等のうち当該領域を所管する情報セキュリティ責任者に許可された者がアクセス可能な領域
2　統括情報セキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定める。
(1)　許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策
(2)　許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策
(区域ごとの対策の決定)
第 43 条　情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び環境に係る対策を行う単位ごとの区域を定める。
2　区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定する。
(要管理対策区域における対策の実施)
第 44 条　区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施する。役職員等及び情報取扱事務従事者が実施すべき対策については、役職員等及び情報取扱事務従事者が認識できる措置を講ずる。
2　区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずる。
3　役職員等及び情報取扱事務従事者は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用する。
4　役職員等及び情報取扱事務従事者が機構外の者を立ち入らせる際には、当該機構外の者にも当該区域で定められた対策に従って利用させる。
第 4 編　外部委託
第 1 章　外部委託
(外部委託に係る規定の整備)
第 45 条　統括情報セキュリティ責任者は、外部委託に係る次の内容を含む規定を整備する。
(1)　委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準
(2)　委託先の選定基準(情報セキュリティ関連個所のみ)

(外部委託に係る契約)
第 46 条　情報セキュリティ責任者は、外部委託を実施する際には、選定基準の情報セキュリティ要件を勘案し、及び選定手続に従って委託先を選定する。
2　委託先の選定に際し、次の内容を含む情報セキュリティ対策を実施することとし、その旨を仕様内容に含める。
(1)　委託先に提供する情報の委託先における目的外利用の禁止
(2)　委託先における情報セキュリティ対策の実施内容及び管理体制
(3)　委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制
(4)　委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報提供
(5)　情報セキュリティインシデントへの対処方法
(6)　情報セキュリティ対策その他の契約の履行状況の確認方法
(7)　情報セキュリティ対策の履行が不十分な場合の対処方法
3　情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含める。
(1)　情報セキュリティ監査の受入れ
(2)　サービスレベルの保証
4　情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、本条第 1 項、第 2 項の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機構に提供し、機構の承認を受けるよう、仕様内容に含める。
(外部委託における対策の実施)
第 47 条　情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認する。
2　情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を役職員等及び情報取扱事務従事者より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく対処を委託先に講じさせる。
3　情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認する。
(外部委託における情報の取扱い)
第 48 条　役職員等及び情報取扱事務従事者は、委託先への情報の提供等において、以下の事項を遵守する。
(1)　委託先に要保護情報を提供する場合は、提供する情報を必要最小限とし、あらかじめ

定められた安全な受渡し方法により提供する。
(2)　提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させる。
(3)　委託業務において、情報セキュリティインシデント、情報の目的外利用等を認知した場合は、速やかに情情報セキュリティ責任者に報告する。
(約款による外部サービスの利用に係る規定の整備)
第 49 条　統括情報セキュリティ責任者は、要機密情報を約款による外部サービスを利用して取り扱わせないよう当該サービスの利用に関する規定を整備する。この場合において、整備する規定には次の内容を含める。
(1)　約款による外部サービスを利用してよい業務の範囲
(2)　業務に利用できる約款による外部サービス
(3)　利用手続及び運用手順
2　情報セキュリティ責任者は、約款による外部サービスを利用する場合は、統括情報セキュリティ責任者の承認を得るとともに、利用するサービスごとの責任者を定める。
(約款による外部サービスの利用における対策の実施)
第 50 条　役職員等及び情報取扱事務従事者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用する。
(ソーシャルメディアサービスによる情報発信時の対策)
第 51 条　統括情報セキュリティ責任者は、機構が管理するアカウントでソーシャルメディアサービスを利用することを前提として、次の内容を含む情報セキュリティ対策に関する運用手順等を定める。
(1)　機構のアカウントによる情報発信が実際の機構のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずる。
(2)　パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずる。
2　前項の場合においては、当該サービスの利用において要機密情報が取り扱われないよう規定する。
3　情報セキュリティ責任者は、機構において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定める。
4　役職員等及び情報取扱事務従事者は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、機構の自己管理ウェブサイトに当該情報を掲載して参照可能とする。
(クラウドサービスの利用における対策)
第 52 条　情報システムセキュリティ責任者は、クラウドサービス(民間事業者が提供するものに限らず、政府が自ら提供するものを含む。以下同じ。)を利用するに当たり、取り扱

う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断する。
2　情報システムセキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定する。
3　情報システムセキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とする。
4　情報システムセキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定める。
5　情報システムセキュリティ責任者は、クラウドサービスに対する第三者機関の情報セキュリティ監査による閲覧可能な報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断する。

第 5 編　情報システムのライフサイクル

第 1 章　情報システムに係る文書等の整備

(情報システム台帳の整備)

第 53 条　統括情報セキュリティ責任者は、原則として、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備する。
2　情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告する。

(情報システム関連文書の整備)

第 54 条　情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、次の内容を網羅した情報システム関連文書を整備する。
(1)　情報システムを構成するサーバ装置及び端末関連情報
(2)　情報システムを構成する通信回線及び通信回線装置関連情報
(3)　情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順
(4)　情報セキュリティインシデントを認知した際の対処手順

(機器等の調達に係る基準の整備)

第 55 条　統括情報セキュリティ責任者は､次の内容を含めた機器等の選定基準を整備する。
(1)　既知の脆弱性に対応していないこと、危殆化した技術を利用していること、不正プログラムを埋め込まれること等のサプライチェーン・リスクへの適切な対処がされていること。
(2)　必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変

更が加えられない管理がなされ、その管理を機構が確認できること。
2　統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備する。
第 2 章　情報システムのライフサイクルの各段階における対策
(実施体制の確保)
第 56 条　情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、情報システムを統括する責任者に求める。
2　情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し、運用管理する組織が定める運用管理規程等に応じた体制の整備を、情報システムを統括する責任者に求める。
(情報システムのセキュリティ要件の策定)
第 57 条　情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム(クラウドサービスを含む。)から分離することの要否を判断した上で、次の内容を含む情報システムのセキュリティ要件を策定する。
(1)　情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件
(2)　情報システム運用時の監視等の運用管理機能要件
(3)　情報システムに関連する脆弱性についての対策要件
2　情報システムセキュリティ責任者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットから様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定する。
3　情報システムセキュリティ責任者は、国民・企業と機構との間で申請及び届出等のオンライン手続を提供するシステムについて、各府省情報化統括責任者(CIO)連絡会議が定める「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づきセキュリティ要件を策定する。
4　情報システムセキュリティ責任者は、機器等を調達する場合には、経済産業省が公表する「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定する。
5　情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程

等に基づいたセキュリティ要件を適切に策定する。

(情報システムの構築を外部委託する場合の対策)

第 58 条　情報システムセキュリティ責任者は､情報システムの構築を外部委託する場合は、次の内容を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させる。

(1)　情報システムのセキュリティ要件の適切な実装

(2)　情報セキュリティの観点に基づく試験の実施

(3)　情報システムの開発環境及び開発工程における情報セキュリティ対策

(情報システムの運用・保守を外部委託する場合の対策)

第 59 条　情報システムセキュリティ責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させる。

(機器等の選定時の対策)

第 60 条　情報システムセキュリティ責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用する。

(情報システムの構築時の対策)

第 61 条　情報システムセキュリティ責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずる。

2　情報システムセキュリティ責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずる。

(納品検査時の対策)

第 62 条　情報システムセキュリティ責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認する。

(情報システムの運用・保守時の対策)

第 63 条　情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用する。

2　情報システムセキュリティ責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し、運用管理する組織との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用する。

3　情報システムセキュリティ責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を

管理する。
(情報システムの更改・廃棄時の対策)
第 64 条　情報システムセキュリティ責任者は､情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずる。
(1)　情報システム更改時の情報の移行作業における情報セキュリティ対策
(2)　情報システム廃棄時の不要な情報の抹消
(情報システムについての対策の見直し)
第 65 条　情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずる。
第 3 章　情報システムの運用継続計画
(情報システムの運用継続計画の整備・整合的運用の確保)
第 66 条　統括情報セキュリティ責任者は、機構において非常時優先業務を支える情報システムの運用継続計画を整備するに当たり、非常時における情報セキュリティに係る対策事項を検討する。
2　統括情報セキュリティ責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認する。
第 6 編　情報システムのセキュリティ要件
第 1 章　情報システムのセキュリティ機能
(主体認証機能の導入)
第 67 条　情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設ける。
2　情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずる。
(識別コード及び主体認証情報の管理)
第 68 条　情報システムセキュリティ責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証を適切に付与し、管理するための措置を講ずる。
2　情報システムセキュリティ責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を講ずる。
(アクセス制御機能の導入)
第 69 条　情報システムセキュリティ責任者は、情報システムが取り扱う情報へのアクセス

を、主体によって制御する必要がある場合、当該情報システムにアクセス制御を行う機能を設ける。

2　情報システムセキュリティ責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用する。

(権限の管理)

第 70 条　情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずる。

2　情報システムセキュリティ責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずる。

(ログの取得・管理)

第 71 条　情報システムセキュリティ責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得する。

2　情報システムセキュリティ責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理する。

3　ログの保存期間は、原則１年とする。

4　情報システムセキュリティ責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施する。

(暗号化機能・電子署名機能の導入)

第 72 条　情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、次の内容の措置を講ずる。

(1)　要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設ける。

(2)　要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設ける。

2　情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会(CRYPTREC)により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、次の事項を含めて定める。

(1)　役職員等及び情報取扱事務従事者が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させる。

(2)　情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用する。
(3)　暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定める。
(4)　暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定める。
3　情報システムセキュリティ責任者は、機構における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤(GPKI)が発行している場合は、それを使用するように定める。
(暗号化・電子署名に係る管理)
第 73 条　情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、次の措置を講ずる。
(1)　電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供する。
(2)　暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、役職員等及び情報取扱事務従事者と共有を図る。
第 2 章　情報セキュリティの脅威への対策
(ソフトウェアに関する脆弱性対策の実施)
第 74 条　情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施する。
2　情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施する。
3　情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずる。
4　情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処する。
(不正プログラム対策の実施)
第 75 条　情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入する。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

2　情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずる。
3　情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行う。
(サービス不能攻撃対策の実施)
第 76 条　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム(インターネットからアクセスを受ける情報システムに限る。以下この条において同じ。)については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行う。
2　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築する。
3　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視を行う。
(標的型攻撃対策の実施)
第 77 条　情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策(入口対策)を講ずる。
2　情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策(内部対策)を講ずる。
第 3 章　アプリケーション・コンテンツの作成・提供
(アプリケーション・コンテンツの作成に係る規程の整備)
第 78 条　統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供時に機構外の情報セキュリティ水準の低下を招く行為を防止するための規程を整備する。
(アプリケーション・コンテンツのセキュリティ要件の策定)
第 79 条　情報システムセキュリティ責任者は、機構外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて次の内容を仕様に含める。
(1)　提供するアプリケーション・コンテンツが不正プログラムを含まない。
(2)　提供するアプリケーションが脆弱性を含まない。
(3)　実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しない。
(4)　電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与える。
(5)　提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの

OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発する。
(6)　サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発する。
2　役職員等及び情報取扱事務従事者は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前項に掲げる内容を調達仕様に含める。
(政府ドメイン名の使用)
第 80 条　情報システムセキュリティ責任者は、機構外向けに提供するウェブサイト等が実際の機構提供のものであることを利用者が確認できるように、政府ドメイン名（以下「機構ドメイン名」という。）を情報システムにおいて使用するよう仕様に含める。ただし、第 52 条 に掲げる場合を除く。
[第 52 条]
2　役職員等及び情報取扱事務従事者は、機構外向けに提供するウェブサイト等の作成を外部委託する場合においては、前項と同様、機構ドメイン名を使用するよう調達仕様に含める。
(不正なウェブサイトへの誘導防止)
第 81 条　情報システムセキュリティ責任者は、利用者が検索サイト等を経由して機構のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずる。
(アプリケーション・コンテンツの告知)
第 82 条　役職員等及び情報取扱事務従事者は、機構外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な対策を講ずる。
2　役職員等及び情報取扱事務従事者は、機構外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つ。
第 7 編　機構の情報システムの構成要素
第 1 章　端末・サーバ装置等
(端末の導入時の対策)
第 83 条　情報システムセキュリティ責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずる。
2　情報システムセキュリティ責任者は、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずる。
3　情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性

が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める。

(端末の運用時の対策)

第 84 条　情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行う。

2　情報システムセキュリティ責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図る。

(端末の運用終了時の対策)

第 85 条　情報システムセキュリティ責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消する。

(サーバ装置の導入時の対策)

第 86 条　情報システムセキュリティ責任者は､要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずる。

2　情報システムセキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保する。

3　情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める。

4　情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずる。

(サーバ装置の運用時の対策)

第 87 条　情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行う。

2　情報システムセキュリティ責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図る。

3　情報システムセキュリティ責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視する措置を講ずる。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

4　情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能になるよう、必要な措置を講ずる。

(サーバ装置の運用終了時の対策)
第 88 条　情報システムセキュリティ責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消する。
(複合機)
第 89 条　情報システムセキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定する。
2　情報システムセキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずる。
3　情報システムセキュリティ責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消する。
(特定用途機器)
第 90 条　情報システムセキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずる。
第 2 章　電子メール・ウェブ等
(電子メールの導入時の対策)
第 91 条　情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定する。
2　情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備える。
3　情報システムセキュリティ責任者は、電子メールのなりすましの防止策を講ずる。
(ウェブサーバの導入・運用時の対策)
第 92 条　情報システムセキュリティ責任者は、ウェブサーバの管理や設定において、次の事項を含む情報セキュリティ確保のための対策を講ずる。
(1)　ウェブサーバが備える機能のうち、不要な機能を停止又は制限する。
(2)　ウェブコンテンツの編集作業を担当する主体を限定する。
(3)　公開してはならない又は無意味なウェブコンテンツが公開されないように管理する。
(4)　ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理する。
(5)　サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設ける。
2　情報システムセキュリティ責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認する。
(ウェブアプリケーションの開発時・運用時の対策)

第 93 条　情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずる。
2　ウェブアプリケーションを運用するときは、前項の対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行う。
(DNS の導入時の対策)
第 94 条　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずる。
2　情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずる。
3　情報システムセキュリティ責任者は、コンテンツサーバにおいて、機構のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずる。
(DNS の運用時の対策)
第 95 条　情報システムセキュリティ責任者は､コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持する。
2　情報システムセキュリティ責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認する。
3　情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずる。
(データベースの導入・運用時の対策)
第 96 条　情報システムセキュリティ責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行う。
2　情報システムセキュリティ責任者は、データベースに格納されているデータにアクセスした利用者を特定できるように、措置を講ずる。
3　情報システムセキュリティ責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずる。
4　情報システムセキュリティ責任者は、データベース及びデータベースにアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずる。
5　情報システムセキュリティ責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をする。
第 3 章　通信回線
(通信回線の導入時の対策)
第 97 条　情報システムセキュリティ責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずる。

2　情報システムセキュリティ責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設ける。
3　情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずる。
4　情報システムセキュリティ責任者は、役職員等及び情報取扱事務従事者が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずる。
5　情報システムセキュリティ責任者は、通信回線装置を要管理対策区域に設置する。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにする。
6　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずる。
7　情報システムセキュリティ責任者は、機構内通信回線にインターネット回線、公衆通信回線等の機構外通信回線を接続する場合には、機構内通信回線及び当該機構内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずる。
8　情報システムセキュリティ責任者は、機構内通信回線と機構外通信回線との間で送受信される通信内容を監視するための措置を講ずる。
9　情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備する。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。
10　情報システムセキュリティ責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保する。
11　情報システムセキュリティ責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておく。
(通信回線の運用時の対策)
第 98 条　情報システムセキュリティ責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずる。
2　情報システムセキュリティ責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行う。
3　情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図る。
4　情報システムセキュリティ責任者は、情報システムの情報セキュリティの確保が困難な

事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更する。

(通信回線の運用終了時の対策)

第 99 条　情報システムセキュリティ責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずる。

(リモートアクセス環境導入時の対策)

第 100 条　情報システムセキュリティ責任者は、役職員等及び情報取扱事務従事者の業務遂行を目的としたリモートアクセス環境を、機構外通信回線を経由して機構の情報システムへリモートアクセスする形態により構築する場合は、VPN 回線を整備するなどして、通信経路及びアクセス先の情報システムのセキュリティを確保する。

(無線 LAN 環境導入時の対策)

第 101 条　情報システムセキュリティ責任者は、無線 LAN 技術を利用して機構内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずる。

(IPv6 通信を行う情報システムに係る対策)

第 102 条　情報システムセキュリティ責任者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づく Phase-2 準拠製品を、可能な場合には選択する。

2　情報システムセキュリティ責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、次の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずる。

(1)　グローバル IP アドレスによる直接の到達性における脅威

(2)　IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

(3)　IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

(4)　アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

(意図しない IPv6 通信の抑止・監視)

第 103 条　情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずる。

第 8 編　情報システムの利用

第 1 章　情報システムの利用

(情報システムの利用に係る規定の整備)

第 104 条　統括情報セキュリティ責任者は、機構の情報システムの利用のうち、情報セキュリティに関する規定を整備する。

2　統括情報セキュリティ責任者は、要保護情報について要管理対策区域外で情報処理を行う場合を想定し、要管理対策区域外に持ち出した端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた安全管理措置に関する規定及び許可手続を定める。

3　統括情報セキュリティ責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定める。

(情報システム利用者の規程の遵守を支援するための対策)

第 105 条　情報システムセキュリティ責任者は、役職員等及び情報取扱事務従事者による規程の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築する。

(情報システムの利用時の基本的対策)

第 106 条　役職員等及び情報取扱事務従事者は、業務の遂行以外の目的で情報システムを利用しない。

2　役職員等及び情報取扱事務従事者は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に機構の情報システムを接続しない。

3　役職員等及び情報取扱事務従事者は、機構内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しない。

4　役職員等及び情報取扱事務従事者は、情報システムで利用を禁止するソフトウェアを利用しない。ただし、情報システムで利用を認めるソフトウェア以外のソフトウェアを業務上の必要により利用する場合は、情報システムセキュリティ責任者の承認を得る。

5　役職員等及び情報取扱事務従事者は、接続が許可されていない機器等を情報システムに接続しない。

6　役職員等及び情報取扱事務従事者は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずる。

7　役職員等及び情報取扱事務従事者は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずる。

8　役職員等及び情報取扱事務従事者は、機密性 3 情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者又は課等情報セキュリティ責任者の許可を得る

(電子メール・ウェブの利用時の対策)

第 107 条　役職員等及び情報取扱事務従事者は、要機密情報を含む電子メールを送受信する場合には、機構が運営し、又は外部委託した電子メールサーバにより提供される電子メ

ールサービスを利用する
2　役職員等及び情報取扱事務従事者は、機構外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に機構ドメイン名を使用する。
3　役職員等及び情報取扱事務従事者は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処する。
4　役職員等及び情報取扱事務従事者は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更をしない。
5　役職員等及び情報取扱事務従事者は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認する。
6　役職員等及び情報取扱事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認する。
(1)　送信内容が暗号化されること
(2)　当該ウェブサイトが送信先として想定している組織のものであること
(識別コード・主体認証情報の取扱い)
第 108 条　役職員等及び情報取扱事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しない。
2　役職員等及び情報取扱事務従事者は、自己に付与された識別コードを適切に管理する。
3　役職員等及び情報取扱事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用する。
4　役職員等及び情報取扱事務従事者は、自己の主体認証情報の管理を徹底する。
(暗号・電子署名の利用時の対策)
第 109 条　役職員等及び情報取扱事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従う。
2　役職員等及び情報取扱事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理する。
3　役職員等及び情報取扱事務従事者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行う。
(不正プログラム感染防止)
第 110 条　役職員等及び情報取扱事務従事者は、不正プログラム感染防止に関する措置に努める。
2　役職員等及び情報取扱事務従事者は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずる。
第 2 章　機構支給以外の端末の利用
(機構支給以外の端末の利用規程の整備・管理)

第 111 条　統括情報セキュリティ責任者は、機構支給以外の端末により業務に係る情報処理を行う場合の許可等の手続に関する手順を定める。
2　統括情報セキュリティ責任者は、要機密情報について機構支給以外の端末により情報処理を行う場合の安全管理措置に関する規程を整備する。
3　情報セキュリティ責任者は、機構支給以外の端末による業務に係る情報処理に関する安全管理措置の実施状況を管理する責任者を定める。
4　前項で定める責任者は、要機密情報を取り扱う機構支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、役職員等及び情報取扱事務従事者に適切に安全管理措置を講じさせる。
(機構支給以外の端末の利用時の対策)
第 112 条　役職員等及び情報取扱事務従事者は、機構支給以外の端末により業務に係る情報処理を行う場合には、前条第 3 項で定める責任者の許可を得る。
2　役職員等及び情報取扱事務従事者は、要機密情報を機構支給以外の端末で取り扱う場合は、課等情報セキュリティ責任者の許可を得る。
3　役職員等及び情報取扱事務従事者は、機構支給以外の端末により業務に係る情報処理を行う場合には、機構にて定められた手続及び安全管理措置に関する規定に従う。
4　役職員等及び情報取扱事務従事者は、情報処理の目的を完了した場合は、要機密情報を機構支給以外の端末から消去する。
附　則
1　この細則は、平成 29 年 4 月 3 日から施行し、平成 29 年 4 月 1 日から適用する。
2　この細則により、細則の実施に係る細目の決定を理事長から授権又は委任される者（以下「授権者」という。）が異なることとなる場合であって、この細則の施行の際、現に制定済の準内部規程等の細目（以下「準内部規程等」という。）があるときは、当該準内部規程等に相当する準内部規程等が新たな授権者により別途制定されるまでの間、現に制定済の準内部規程等を当該新たな授権者により制定されたものとみなす。

〇個人情報保護に関する実施細則

（平成 17 年 4 月 1 日細則(総)第 11 号）

改正　平成 20 年 4 月 1 日細則(総)第 5 号 平成 20 年 11 月 14 日細則 (情) 第 51 号
平成 21 年 3 月 16 日細則(情)第 8 号 平成 22 年 6 月 28 日細則(情)第 33 号
平成 23 年 3 月 31 日細則(情)第 9 号 平成 23 年 12 月 12 日細則(情)第 49 号
平成 27 年 6 月 12 日細則(情)第 13 号 平成 27 年 9 月 30 日細則(情)第 20 号
平成 29 年 5 月 2 日細則(情)第 12 号

目次

第 1 章　総則(第 1 条・第 2 条)
第 2 章　個人情報保護の体制(第 3 条－第 7 条)
第 3 章　役職員等及び情報取扱事務従事者の責務(第 8 条)
第 4 章　個人情報及び特定個人情報等の取扱い(第 9 条－第 21 条)
第 5 章　情報システム等における安全の確保等(第 22 条)
第 6 章　保有個人情報等の取扱いに係る業務の委託等(第 23 条・第 24 条)
第 7 章　個人情報ファイル簿の作成及び公表(第 25 条)
第 8 章　保有個人情報等の開示、訂正及び利用停止(第 26 条)
第 9 章　独立行政法人等非識別加工情報の提供(第 27 条－第 40 条)
第 10 章　安全管理上の問題への対応(第 41 条)
第 11 章　教育研修(第 42 条)
第 12 章　監査及び点検の実施(第 43 条－第 45 条)
第 13 章　行政機関との連携(第 46 条)
第 14 章　雑則(第 47 条)
附則

第 1 章　総則

(目的)

第 1 条　この細則は、独立行政法人国際協力機構情報セキュリティ管理規程(平成 29 年規程(情)第 14 号。以下「管理規程」という。)第 24 条の規定、独立行政法人等の保有する個人情報の保護に関する法律(平成 15 年法律第 59 号。以下「法」という。)及び行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」という。）に基づき、独立行政法人国際協力機構(以下「機構」という。)における個人情報及び特定個人情報等の取扱いに関する基本的事項を定めるものとする。[独立行政法人国際協力機構情報セキュリティ管理規程(平成 17 年規程(総)第 6 号。以下「管理規程」という。)第 22 条] [独立行政法人等の保有する個人情報の保護に関する法律(平

成 15 年法律第 59 号。以下「個人情報保護法」という。)]

(用語の定義)

第 2 条　この細則における用語の意義は、それぞれ当該各号に定めるところによる。なお、本条の各号において定めのない用語の意義については、法第 2 条及び番号法第 2 条の定めるところによる。

(1)　個人情報　生存する個人に関する情報であって、次に掲げるものをいう。

イ　当該情報に含まれる氏名、生年月日その他の記述等(文書、図面若しくは電磁的記録(電磁的方式(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。以下同じ。)で作られた記録をいう。)に記載され、若しくは記録された、又は音声、動作その他の方法を用いて表された一切の事項(個人識別符号を除く。)をいう。以下同じ。)により特定の個人を識別することができるもの(他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。)

ロ　個人識別符号が含まれるもの

(2)　個人識別符号　次のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。

イ　特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの

ロ　個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式に記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

(3)　保有個人情報　機構の役員又は職員が職務上作成し、又は取得した個人情報であって、役員又は職員が組織的に利用するものとして、機構が保有しているものをいう。ただし、独立行政法人等の保有する情報の公開に関する法律(平成 13 年法律第 140 号、以下「独立行政法人等情報公開法」という。)第 2 条第 2 項に規定する法人文書(同項第 3 号に掲げるものを含む。以下単に「法人文書」という。)に記録されているものに限る。

[独立行政法人等の保有する情報の公開に関する法律(平成 13 年法律第 140 号)第 2 条第 2 項]

(4)　個人情報ファイル　保有個人情報を含む情報の集合物であって、次に掲げるものをいう。

イ　一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

ロ　イに掲げるもののほか、一定の事務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索することができるように体系的に構成したもの

(5)　個人番号　住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。
(6)　本人　個人情報及び個人番号によって識別される特定の個人をいう。
(7)　情報システム　管理規程第１条第３項第１号に規定する情報システムをいう。
[管理規程第３条第２号]
(8)　情報セキュリティ管理細則(平成29年細則(情)第11号。以下「管理細則」という。)第２条第２号に規定する部等をいう。
[管理規程第３条第10号]
(9)　役職員等　管理規程第２条第１号に規定する役職員等をいう。
[管理規程第３条第11号]
(10)　情報取扱事務従事者　管理規程第２条第２号に規定する情報取扱事務従事者をいう。
(11)　独立行政法人等　法第２条第１項に規定する独立行政法人等をいう。
[個人情報保護法第２条第１項]
(12)　特定個人情報　個人番号(個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。)をその内容に含む個人情報をいう。
(13)　特定個人情報ファイル　個人番号をその内容に含む個人情報ファイルをいう。
(14)　個人番号関係事務　個人番号利用事務に関して行われる他人の個人番号を必要な限度で利用して行う事務をいう。
(15)　個人番号関係事務実施者　個人番号関係事務を処理する者及び個人番号関係事務の全部又は一部の委託を受けた者をいう。
(16)　非識別加工情報　個人情報(他の情報と照合することができ、それにより特定の個人を識別することができることとなるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを除く。)を除く。以下この項において同じ。)の区分に応じて法第２条第８項各号に定める措置を講じて特定の個人を識別することができない(個人に関する情報について、当該個人に関する情報に含まれる記述等により、又は当該個人に関する情報が他の情報と照合することができる個人に関する情報である場合にあっては他の情報(当該個人に関する情報の全部又は一部を含む個人情報その他国の個人情報保護委員会規則（以下、「規則」という。）で定める情報を除く。)と照合することにより、特定の個人を識別することができないことをいう。)ように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。
(17)　独立行政法人等非識別加工情報　法第２条第９項各号に該当する個人情報ファイルを構成する保有個人情報(他の情報と照合することができ、それにより特定の個人を識別することができることとなるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを除く。)を除く。)の全部又は一部(これらの

一部に独立行政法人等情報公開法第５条に規定する不開示情報（同条第１号に掲げる情報を除く。）が含まれているときは、当該不開示情報に該当する部分を除く。）を加工して得られる非識別加工情報をいう。

(18)　独立行政法人等非識別加工情報ファイル　独立行政法人等非識別加工情報を含む情報の集合物であって、検索することができるように体系的に構成したものをいう。

(19)　独立行政法人等非識別加工情報取扱事業者　独立行政法人等非識別加工情報ファイルを事業の用に供している者(ただし、国の機関、独立行政法人等、地方公共団体、地方独立行政法人(地方独立行政法人法(平成15年法律第118号）第２条第１項に規定する地方独立行政法人をいう。以下同じ。）を除く。）をいう。

(20)　独立行政法人等非識別加工情報等　独立行政法人等非識別加工情報、独立行政法人等非識別加工情報の作成に用いた保有個人情報から削除した記述等及び個人識別符号並びに第35条により行った加工の方法に関する情報をいう。

第２章　個人情報保護の体制

(個人情報保護管理体制の整備)

第３条　機構における個人情報保護体制を確保するための管理体制は、管理規程第５条、及び管理細則第12条に定めるところによる。

[管理規程第４条]

(最高情報セキュリティ責任者等)

第４条　最高情報セキュリティ責任者（以下「最高責任者」という。）は、管理規程第５条に定めるところにより、機構の保有個人情報及び個人番号(以下「保有個人情報等」という。)の管理に関する事務を総括する。

[管理規程第５条]

２　統括情報セキュリティ責任者(以下「統括責任者」という。)は、管理細則第12条第２項に定めるところにより、最高責任者を補佐し、関係事務を総括整理する。

[管理規程第６条]

３　情報セキュリティ責任者(以下「責任者」という。)は、管理細則第12条第１項に定めるところにより、各部等の保有個人情報等の適切な管理を確保する任にあたる。

[管理規程第７条]

４　責任者は、保有個人情報等を主管している情報システムで取り扱う場合、情報システム管理規程第９条に定める当該情報システムのシステム管理責任者と連携して、その任にあたる。

５　課等情報セキュリティ責任者(以下「課等責任者」という。)は、管理細則第12条第３項に定めるところにより、責任者の命を受けて、当該課における保有個人情報等を適切に管理する任にあたる。

[管理規程第８条]

６　責任者は、個人番号及び特定個人情報（以下「特定個人情報等」という。）を取り扱う

役職員等（以下「事務取扱担当者」という。）並びにその役割を指定し、各事務取扱担当者が取り扱う特定個人情報等の範囲を指定する。

(監査責任者)

第 5 条　機構は監査責任者を一人置くこととし、監査室長をもってその任に充てる。監査責任者は、保有個人情報等の管理状況について監査する。

(個人情報保護委員会)

第 6 条　機構に個人情報保護委員会(以下「委員会」という。)を置く。

2　委員会は、機構の保有個人情報等の管理に係る重要事項について審議するとともにその他の必要事項の報告を受ける。

3　委員会の構成は、管理規程第 6 条第 2 項に定めるところによる。ただし、委員会の委員は、管理規程第 6 条第 2 項第 3 号に定める情報セキュリティ委員会の委員に加えて、国内事業部長、調達部長、国際協力人材部長及び青年海外協力隊事務局長をもって構成する。

[管理規程第 10 条第 2 項] [管理規程第 10 条第 2 項第 3 号]

4　委員会は、必要に応じ、他の役職員等若しくは第三者の専門家(以下「専門家」という。)から委員会の実施する内容に関連し適宜助言を受けること又は専門家を委員会に出席させることができる。

5　委員会は、事務局を情報システム室計画課に置き、計画課長を事務局長とする。

6　委員会は、定期的及び委員長が必要と認めたとき随時招集し、これを開催する。

7　委員会の実施する内容に関連し、必要に応じ、適宜、専門家による助言を受けるものとする。

8　議事の運営は、委員長がこれにあたる。ただし、委員長が必要と認めるときは、副委員長に委員会の運営の一部を代行させることができる。

9　委員長に事故あるときは、副委員長に委員会の運営を代行させることができる。

10　前 2 項により副委員長が一部若しくは全部の運営を代行した場合、副委員長は委員会終了後速やかにその結果を委員長に報告するものとする。

11　委員長、副委員長又は事務局長は、委員会での検討及び審議の結果を理事長に報告するものとする。

(個人情報相談窓口)

第 7 条　法に基づく開示、訂正、利用停止請求、及びその他相談、並びに独立行政法人等非識別加工情報の提供等に対応する窓口として、個人情報相談窓口を設置する。

[個人情報保護法]

2　個人情報相談窓口は、法人文書の開示等の手続きに関する実施細則(平成 15 年細則(総)第 2 号)第 4 条に定める情報公開窓口が兼ねる。

[法人文書の開示等の手続きに関する実施細則(平成 15 年細則(総)第 2 号)第 4 条]

3　個人情報相談窓口を設置する部門の長は、本部の個人情報相談窓口において、開示、訂正、利用停止請求、相談等に対応する個人情報相談窓口担当者を指名する。

第 3 章　役職員等及び情報取扱事務従事者の責務

(役職員等及び情報取扱事務従事者の責務)

第 8 条　役職員等及び情報取扱事務従事者は、法及び番号法の趣旨に則り、関連する法令並びにこの細則等の定め及び第 4 条に掲げる者の指示に従い、保有個人情報等を取り扱わなければならない。

[個人情報保護法] [第 4 条]

2　役職員等及び情報取扱事務従事者は、次に掲げる行為を行ってはならない。

(1)　その業務に関して知り得た個人情報、特定個人情報等及び独立行政法人等非識別加工情報等の内容をみだりに他人に知らせ、又は不当な目的に利用すること。

(2)　その職権を濫用して、専らその職務の用以外の用に供する目的で個人の秘密に属する事項が記録された文書、図画又は電磁的記録を収集すること。

3　前項の規定は、役職員等及び情報取扱事務従事者がその職を退いた後について準用する。

第 4 章　個人情報及び特定個人情報等の取扱い

(個人情報の保有の制限等)

第 9 条　個人情報を保有するに当たっては、法令の定める業務を遂行するため必要な場合に限り、かつ、その利用の目的をできる限り特定しなければならない。

2　前項の規定により特定された利用の目的(以下「利用目的」という。)の達成に必要な範囲を超えて、個人情報を保有してはならない。

3　利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

4　次に掲げる個人情報は「要配慮個人情報」とし、その保有等を行わないものとする。ただし、明示的な本人の同意又は法令に特別の規定がある場合、司法手続上必要不可欠である場合、その他個人情報を取り扱う事務の目的を達成するために当該個人情報が必要かつ欠くことができない場合は、この限りではない。

(1)　本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして次の各号に掲げる記述が含まれる個人情報をいう。

(2)　身体障害、知的障害、精神障害（発達障害を含む。）等の心身の機能の障害があること。

(3)　本人に対して医師等により行われた疾病の予防及び早期発見のための健康診断等の結果。

(4)　健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと。

(5)　本人を被疑者又は被告人として、逮捕、捜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと。

(6)　本人を少年法第３条第１項に規定する少年又はその疑いがある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと。

(利用目的の明示)

第 10 条　本人から直接書面（電磁的記録を含む。）に記録された当該本人の個人情報を取得するときは、次に掲げる場合を除き、あらかじめ、本人に対し、その利用目的を明示しなければならない。

(1)　人の生命、身体又は財産の保護のために緊急に必要があるとき。

(2)　利用目的を本人に明示することにより、本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるとき。

(3)　利用目的を本人に明示することにより、国の機関、独立行政法人等又は地方公共団体が行う事務又は事業の適正な遂行に支障を及ぼすおそれがあるとき。

(4)　取得の状況からみて利用目的が明らかであると認められるとき。

(適正な取得)

第 11 条　役職員等及び情報取扱事務従事者は、偽りその他不正の手段により個人情報を取得してはならない。

(特定個人情報等の利用の制限等)

第 12 条　責任者は、特定個人情報等の利用にあたり、次の内容を遵守する。

(1)　個人番号の利用は、番号法があらかじめ限定的に定めた事務に限定する。

(2)　個人番号関係事務を処理するために必要な場合を除き、個人番号の提供を求めてはならない。

(3)　個人番号関係事務を処理するために必要な場合その他番号法で定める場合を除き、特定個人情報ファイルを作成してはならない。

(4)　特定個人情報ファイルを保有する場合は、保有する前に特定個人情報保護評価を実施しなければならない。なお、番号法第 26 条第１項に基づく特定個人情報保護評価指針において特定個人情報保護評価の実施が義務付けられない事務は除く。

(5)　番号法第 19 条各号のいずれかに該当する場合を除き、他人の特定個人番号等を収集又は保管してはならない。

(正確性の確保)

第 13 条　役職員等及び情報取扱事務従事者は、利用目的の達成に必要な範囲内で、保有個人情報等が過去又は現在の事実と合致するよう努めなければならない。

2　役職員等及び情報取扱事務従事者は、保有個人情報等の内容に誤り等を発見した場合には、管理責任者の指示に従い、訂正等を行う。

(アクセス制限)

第 14 条　課等責任者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等にアクセスする権限を有する役職員等及び情報取扱事務従事者とその権限の内容を、当該役職員等及び情報取扱事務従事者が業務を行う上で必要最小限の範囲に限定する。

2　アクセス権限を有しない役職員等及び情報取扱事務従事者は、保有個人情報等にアクセスしてはならない。
3　アクセス権限を有する役職員等及び情報取扱事務従事者であっても、業務上の目的以外の目的で保有個人情報等にアクセスしてはならない。
(パスワード・暗号化)
第 15 条　統括責任者は、電磁的記録について、保有個人情報等の秘匿性等その内容に応じて、パスワードの設定、その暗号化のために必要な措置を講ずる。
2　役職員等及び情報取扱事務従事者は、上記に基づき、処理する保有個人情報等について、当該保有個人情報等の秘匿性等その内容に応じて、適切に暗号化を行う。
(複製等の制限)
第 16 条　役職員等及び情報取扱事務従事者が、業務上の目的で保有個人情報等を取り扱う場合であっても、課等責任者は、次に掲げる行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を限定し、役職員等及び情報取扱事務従事者は課等責任者の指示に従い行う。
(1)　保有個人情報等の複製
(2)　保有個人情報等の送信
(3)　保有個人情報等が記録されている媒体の外部への送付又は持出し
(4)　その他保有個人情報等の適切な管理に支障を及ぼすおそれのある行為
(媒体の管理)
第 17 条　役職員等及び情報取扱事務従事者は、課等責任者の指示に従い、保有個人情報等が記録されている媒体を管理細則第 43 条に基づき決定する物理的セキュリティレベル 3 の領域にて、業務終了後に施錠保管する。また、必要があると認めるときは、耐火金庫への保管等を行う。
(廃棄)
第 18 条　役職員等及び情報取扱事務従事者は、法人文書管理規程に基づく保存期間が満了した保有個人情報等又は保有個人情報等が記録されている媒体(端末及びサーバに内蔵されているものを含む。)について、課等責任者の指示に従い、当該保有個人情報等の復元不可能な方法により当該保有個人情報等の消去又は当該媒体の廃棄を行う。
(利用目的外の利用及び提供)
第 19 条　役職員等及び情報取扱事務従事者は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報等を利用し、又は提供してはならない。
2　前項の規定にかかわらず、課等責任者が次の各号のいずれかに該当すると認めるときは、役職員等及び情報取扱事務従事者は利用目的以外の目的のために保有個人情報を利用することができる。ただし、保有個人情報を利用目的以外の目的のために利用することによって、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。

(1)　本人の同意があるとき。
(2)　法令の定める業務の遂行に必要な限度で保有個人情報を内部で利用する場合であって、当該保有個人情報を利用することについて相当な理由のあるとき。
3　前項の規定に基づき、保有個人情報を利用する場合には、課等責任者は、個人の権利利益を保護するため特に必要があると認めるときは、保有個人情報の利用目的以外の目的のための機構内における利用を特定の役員又は職員に限るものとする。
4　第 1 項の規定にかかわらず、責任者が次の各号のいずれかに該当すると認めるときは、課等責任者は利用目的以外の目的のために保有個人情報を提供することができる。ただし、保有個人情報を利用目的以外の目的のために提供することによって、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。
(1)　本人の同意があるとき、又は本人に提供するとき。
(2)　行政機関(行政機関の保有する個人情報の保護に関する法律(平成 15 年法律第 58 号)第 2 条第 1 項に規定する行政機関をいう。以下同じ。)、他の独立行政法人等又は地方公共団体に保有個人情報を提供する場合において、保有個人情報の提供を受ける者が、法令の定める事務又は業務の遂行に必要な限度で提供に係る個人情報を利用し、かつ、当該個人情報を利用することについて相当な理由のあるとき。
[行政機関の保有する個人情報の保護に関する法律(平成 15 年法律第 58 号)第 2 条第 1 項]
(3)　前 2 号に掲げる場合のほか、専ら統計の作成又は学術研究の目的のために保有個人情報を提供するとき、本人以外の者に提供することが明らかに本人の利益になるとき、その他保有個人情報を提供することについて特別の理由のあるとき。
5　前 2 項の規定は、保有個人情報の利用又は提供を制限する他の法令の規定の適用を妨げるものではない。
6　責任者は、番号法第 19 条各号のいずれかに該当する場合を除き、特定個人情報を提供してはならない。
(保有個人情報の利用目的外の提供を受ける者に対する措置要求)
第 20 条　課等責任者は、前条第 4 項第 2 号又は第 3 号の規定に基づき、行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について書面を取り交わすものとする。
2　課等責任者は、前条第 4 項第 2 号又は第 3 号の規定に基づき、行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求しなければならない。必要があると認めるときは、提供前又は随時に実地の調査等を行い措置状況を確認し、その結果を記録するとともに、改善要求等の措置を講ずるものとする。
3　課等責任者は、前条第 4 項第 2 号の規定に基づき、行政機関又は独立行政法人等に保有個人情報を提供する場合において、必要があると認めるときは、前 2 項に規定する措置を講ずるものとする。第 1 項の書面の取り交わしを行わない場合は、課等責任者は、保有個

人情報を提供したことについて、記録しなければならない。
(保有個人情報等の取扱状況の記録)
第 21 条　課等責任者は､保有個人情報等の秘匿性等その内容に応じて､台帳等を整備して、当該保有個人情報等の利用及び保管等の取扱いの状況について記録する。
第 5 章　情報システム等における安全の確保等
(情報システム等における安全の確保等)
第 22 条　情報システムにおける安全の確保等及び保有個人情報等を取り扱う基幹的なサーバ等の機器を設置する室等の安全管理に関しては、管理規程及び管理細則の定めるところによる。その際は保有個人情報等の秘匿性等重要度に応じて必要な措置を講ずるものとする。
[管理規程] [情報セキュリティ管理細則（平成 20 年細則（情）第 39 号）]
第 6 章　保有個人情報等の取扱いに係る業務の委託等
(業務の委託等)
第 23 条　責任者は、保有個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講ずるものとする。
2　責任者は、保有個人情報の取扱いに係る業務を外部に委託する場合には、契約書に、次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理、実施体制並びに個人情報の管理状況についての検査に関する事項等の必要な事項について書面で確認する。
(1)　個人情報の安全確保の措置
(2)　個人情報に関する秘密保持、目的外利用の禁止等の義務
(3)　再委託の制限又は事前承認等再委託に係る条件に関する事項
(4)　個人情報の複製等の制限に関する事項
(5)　個人情報の漏えい等の事案の発生時における対応に関する事項
(6)　委託終了時における個人情報の消去及び媒体の返却に関する事項
(7)　前各号に違反した場合における契約の解除権、損害賠償責任その他必要な事項
3　課等責任者は、保有個人情報等の取扱いに係る業務を外部に委託する場合には、委託する保有個人情報等の秘匿性等その内容に応じて、委託先における個人情報の管理の状況について、年 1 回以上の定期的検査等により確認し、その結果を記録するとともに、改善要求等の措置を講ずるものとする。
4　委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に第 2 項の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は機構自らが前項の措置を実施する。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。
5　派遣先責任者(労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等

に関する法律(昭和 60 年法律第 88 条)第 41 条に規定する者をいう。)は、保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等、個人情報の取扱いに関する事項を明記しなければならない。
[労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律(昭和 60 年法律第 88 条)第 41 条]
(個人番号関係事務の委託)
第 24 条　責任者は個人番号関係事務の全部又は一部を委託する場合には、前条の措置に加えて次の各号に掲げる措置についても講ずるものとする。
(1)　委託先において、番号法に基づき機構が果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認する。
(2)　委託先において、機構が果たすべき安全管理措置と同等の措置が講じられているよう必要かつ適切な措置を行う。
(3)　委託先が当該業務を再委託する際には、委託する個人番号関係事務において取り扱う特定個人情報等の適切な安全管理が図られることを確認した上で再委託の諾否を判断する。
第 7 章　個人情報ファイル簿の作成及び公表
(個人情報ファイル簿の作成及び公表)
第 25 条　第 6 条第 5 項における事務局(以下この条において「事務局」という。)は、機構が個人情報ファイル(特定個人情報ファイルを含む。第 7 項各号に掲げるもの及び第 8 項の規定により個人情報ファイル簿に掲載しないものを除く。以下第 2 項において同じ。)を保有するに至ったときは、それぞれ第 6 項に掲げる事項を記載した帳簿(以下「個人情報ファイル簿」という。)を直ちに作成しなければならない。
[第 6 条第 4 項]
2　個人情報ファイル簿は、機構が保有している個人情報ファイルを通じて一の帳簿とする。
3　個人情報ファイル簿に記載すべき事項に変更があったときは、当該個人情報を管理する課等責任者は直ちに事務局にその旨報告しなければならない。事務局は、報告があったときは直ちに、当該個人情報ファイル簿を修正しなければならない。
4　機構が個人情報ファイル簿に掲載した個人情報ファイルの保有をやめたとき、又はその個人情報ファイルが第 7 項第 7 号に該当するに至ったときは、当該個人情報を管理する課等責任者は、遅滞なく、事務局に報告しなければならない。事務局は、報告があったときは、遅滞なく、当該個人情報ファイルについての記載を消除しなければならない。
5　事務局は、個人情報ファイル簿を作成したときは、遅滞なく、これを機構に備えて置き一般の閲覧に供するとともに、インターネットの利用その他の情報通信の技術を利用する方法により公表しなければならない。
6　事務局は、機構が保有している個人情報ファイルについて、それぞれ次に掲げる事項を記載した個人情報ファイル簿を作成し、公表しなければならない。
(1)　個人情報ファイルの名称

(2)　機構の名称及び個人情報ファイルが利用に供される事務をつかさどる組織の名称
(3)　個人情報ファイルの利用目的
(4)　個人情報ファイルに記録される項目(以下この条において「記録項目」という。)及び本人(他の個人の氏名、生年月日その他の記述等によらないで検索し得る者に限る。次項第7号において同じ。)として個人情報ファイルに記録される個人の範囲(以下この条において「記録範囲」という。)
(5)　個人情報ファイルに記録される個人情報(以下この条において「記録情報」という。)の収集方法
(6)　記録情報を機構以外のものに経常的に提供する場合には、その提供先
(7)　次条に定める請求を受理する組織の名称及び所在地
(8)　法第27条第1項ただし書又は第36条第1項ただし書に該当するときは、その旨
[個人情報保護法第27条第1項]［第36条第1項]
(9)　第2条第3号イに係る個人情報ファイル又は同号ロに係る個人情報ファイルの別
[第2条第3号]
(10)　第2条第3号イに係る個人情報ファイルについて、次項第10号に規定する個人情報ファイルがあるときは、その旨
[第2条第3号]
(11)　　記録情報に要配慮個人情報が含まれるときは、その旨
(12)　　その他政令で定める事項
7　前項の規定は、次に掲げる個人情報ファイルについては、適用しない。
(1)　役員若しくは職員又はこれらの職にあった者に係る個人情報ファイルであって、専らその人事、給与若しくは福利厚生に関する事項又はこれらに準ずる事項を記録するもの(職員の採用試験に関する個人情報ファイルを含む。)
(2)　専ら試験的な電子計算機処理の用に供するための個人情報ファイル
(3)　前項の規定による公表に係る個人情報ファイルに記録されている記録情報の全部又は一部を記録した個人情報ファイルであって、その利用目的、記録項目及び記録範囲が当該公表に係るこれらの事項の範囲内のもの
(4)　一年以内に消去することとなる記録情報のみを記録する個人情報ファイル
(5)　資料その他の物品若しくは金銭の送付又は業務上必要な連絡のために利用する記録情報を記録した個人情報ファイルであって、送付又は連絡の相手方の氏名、住所その他の送付又は連絡に必要な事項のみを記録するもの
(6)　役員又は職員が学術研究の用に供するためその発意に基づき作成し、又は取得する個人情報ファイルであって、記録情報を専ら当該学術研究の目的のために利用するもの
(7)　本人の数が千人に満たない個人情報ファイル
(8)　次のいずれかに該当する者に係る個人情報ファイルであって、専らその人事、給与若しくは福利厚生に関する事項又はこれらに準ずる事項を記録するもの(イに掲げる者の採

用のための試験に関する個人情報ファイルを含む。）
イ　行政機関が雇い入れる者であって国以外のもののために労務に服するもの
ロ　イに掲げる者であった者
ハ　第１号に規定する者又はイ若しくはロに掲げる者の被扶養者又は遺族
(9)　第１号に規定する者及び前号イからハまでに掲げる者を併せて記録する個人情報ファイルであって、専らその人事、給与若しくは福利厚生に関する事項又はこれらに準ずる事項を記録するもの
(10)　第２条第３号ロに係る個人情報ファイルで、その利用目的及び記録範囲が第６項の規定による公表に係る第２条第３号イに係る個人情報ファイルの利用目的及び記録範囲の範囲内であるもの
[第２条第３号]［第２条第３号]
(11)　独立行政法人等非識別加工情報ファイルに該当する個人情報ファイル
(12)　記録情報に削除情報が含まれる個人情報ファイル
8　第６項の規定にかかわらず、事務局は、記録項目の一部若しくは同項第５号若しくは第６号に掲げる事項を個人情報ファイル簿に記載し、又は個人情報ファイルを個人情報ファイル簿に掲載することにより、利用目的に係る事務又は事業の性質上、当該事務又は事業の適正な遂行に著しい支障を及ぼすおそれがあると認めるときは、その記録項目の一部若しくは事項を記載せず、又はその個人情報ファイルを個人情報ファイル簿に掲載しないことができる。
第８章　保有個人情報等の開示、訂正及び利用停止
(開示、訂正及び利用停止)
第 26 条　機構は、本人(未成年者又は成年被後見人が本人の場合は、その法定代理人を含む。)から保有個人情報等の開示、訂正又は利用停止の請求を受けた場合は、独立行政法人法の趣旨に則り、当該請求への対応を行う。
[個人情報保護法]
2　本人からの請求の受理その他開示等の実施に必要な手続は、別途定めるものとする。
第９章　独立行政法人等非識別加工情報の提供
(独立行政法人等非識別加工情報の作成及び提供等)
第 27 条　機構は、独立行政法人等非識別加工情報(独立行政法人等非識別加工情報ファイルを構成するものに限る。)を作成し、提供することができる。
2　　機構は、法令に基づく場合を除き、利用目的以外の目的のために独立行政法人等非識別加工情報及び削除情報（保有個人情報に該当するものに限る。）を自ら利用し、又は提供してはならない。
3　前項の「削除情報」とは、独立行政法人等非識別加工情報の作成に用いた保有個人情報(他の情報と照合することができ、それにより特定の個人を識別することができることとなるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することがで

きることとなるものを除く。)を除く。以下この章において同じ。)から削除した記述等及び個人識別符号をいう。

(提案の募集に関する事項の個人情報ファイル簿への記載)

第 28 条　機構は、保有している個人情報ファイルが法第 2 条第 9 項各号のいずれにも該当すると認めるときは、当該個人情報ファイルについては、個人情報ファイル簿に次に掲げる事項を記載しなければならない。

(1)　提案の募集をする個人情報ファイルであること

(2)　提案を受ける組織の名称及び所在地

(3)　当該個人情報ファイルが法第 2 条第 9 項第 2 号（ロに係る部分に限る）に該当するときは、意見書の提出の機会が与えられること

(提案の募集)

第 29 条　機構は、機構が保有している個人情報ファイル(個人情報ファイル簿に前条第 1 号に掲げる事項の記載があるものに限る。)について、次条第 1 項の提案を募集するものとする。

(独立行政法人等非識別加工情報をその用に供して行う事業に関する提案)

第 30 条　前条の規定による募集に応じて、独立行政法人等非識別加工情報をその事業の用に供する独立行政法人等非識別加工情報取扱事業者になろうとする者は、機構に対し当該事業に関する提案をすることができる。

2　前項の提案は、規則で定める事項を記載した書面を機構に提出する。

3　前項の書面には、次に掲げる書面その他規則で定める書類を添付しなければならない。

(1)　第 1 項の提案をする者が次条各号のいずれにも該当しないことを誓約する書面

(2)　前項第 5 号の事業が新たな産業の創出又は活力ある経済社会若しくは豊かな国民生活の実現に資するものであることを明らかにする書面

(欠格事由)

第 31 条　次の各号のいずれかに該当する者は、前条第 1 項の提案をすることができない。

(1)　未成年者、成年被後見人又は被保佐人

(2)　破産手続開始の決定を受けて復権を得ない者

(3)　禁錮以上の刑に処せられ、又は個人情報の保護に関する法律（平成 15 年法律第 57 号）若しくは行政機関の保有する個人情報の保護に関する法律(平成 15 年法律第 58 号。以下「行政法」という。)の規定により刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から起算して 2 年を経過しない者

(4)　第 39 条により独立行政法人等非識別加工情報の利用に関する契約を解除され、その解除の日から起算して 2 年を経過しない者

(5)　行政法第 44 条の 14 の規定により行政法第 2 条第 9 項に規定する行政機関非識別加工情報（同条第 10 項に規定する行政機関非識別加工情報ファイルを構成するものに限る。）の利用に関する契約を解除され、その解除の日から起算して 2 年を経過しない者

(6)　法人その他の団体であって、その役員のうちに前各号のいずれかに該当する者があるもの

(提案の審査等)

第 32 条　機構は、第 30 条の提案があったときは、当該提案が次に掲げる基準に適合するかどうかを審査しなければならない。

(1)　第 30 条第 1 項の提案をした者が前条各号のいずれにも該当しない。

(2)　第 30 条第 2 項第 3 号の提案に係る独立行政法人等非識別加工情報の本人の数が千人以上であり、かつ、提案に係る個人情報ファイルを構成する保有個人情報の本人の数以下である。

(3)　第 30 条第 2 項第 3 号及び第 4 号に掲げる事項により特定される加工の方法が第 35 条第 1 項の基準に適合するものである。

(4)　第 30 条第 2 項第 5 号の事業が新たな産業の創出又は活力ある経済社会若しくは豊かな国民生活の実現に資するものである。

(5)　第 30 条第 2 項第 6 号の期間が独立行政法人等非識別加工情報の効果的な活用の観点から、事業の目的、内容並びに独立行政法人等非識別加工情報の利用の目的及び方法からみて必要な期間を超えないものである。

(6)　第 30 条第 2 項第 5 号の提案に係る独立行政法人等非識別加工情報の利用の目的及び方法並びに同項第 7 号の措置が当該独立行政法人等非識別加工情報の本人の権利利益を保護するために適切なものである。

(7)　前各号に掲げるもののほか、機構が独立行政法人等非識別加工情報を作成する場合に機構の業務の遂行に著しい支障を及ぼさないものである。

2　機構は、前項の規定により審査した結果、第 30 条第 1 項の提案が前項各号に掲げる基準に適合すると認めるときは、規則で定める審査結果通知書に独立行政法人等非識別加工情報の利用に関する契約締結の申し込みに係る書類を添えて、当該提案をした者に対し、次に掲げる事項を通知するものとする。

(1)　第 34 条の規定により独立行政法人等との間で独立行政法人等非識別加工情報の利用に関する契約を締結することができる旨

(2)　前号に掲げるもののほか、規則で定める事項

3　機構は、第 1 項の規定により審査した結果、第 30 条第 1 項の提案が第 1 項各号に掲げる基準のいずれかに適合しないと認めるときは、規則で定める審査結果通知書により、当該提案をした者に対し、理由を付して、その旨を通知するものとする。

(第三者に対する意見書提出の機会の付与等)

第 33 条　個人情報ファイル簿に第 28 条第 3 号に掲げる事項の記載がある個人情報ファイルに係る第 30 条第 1 項の提案については、当該提案を当該提案に係る個人情報ファイルを構成する保有個人情報が記録されている法人文書の独立行政法人等情報公開法第 3 条の規定による開示の請求と、前条第 2 項の規定による通知を当該法人文書の全部又は一部を開

示する旨の決定とみなして、独立行政法人等情報公開法第 14 条第 1 項及び第 2 項の規定を準用する。

2　前項において準用する独立行政法人等情報公開法第 14 条第 1 項又は第 2 項の規定により意見書の提出の機会を与えられた同条第 1 項に規定する第三者が第 30 条第 1 項の提案に係る独立行政法人等非識別加工情報の作成に反対の意思を表示した意見書を提出したときは、当該提案に係る個人情報ファイルから当該第三者を本人とする保有個人情報を除いた部分を当該提案に係る個人情報ファイルとみなして、この章の規定を適用する。

(独立行政法人等非識別加工情報の利用に関する契約の締結)

第 34 条　第 32 条第 2 項の規定による通知を受けた者は、同条第 2 項の書類を提出することにより、機構との間で、独立行政法人等非識別加工情報の利用に関する契約を締結することができる。

(独立行政法人等非識別加工情報の作成等)

第 35 条　機構は、独立行政法人等非識別加工情報を作成するときは、特定の個人を識別することができないように及びその作成に用いる保有個人情報を復元することができないようにするために必要なものとして規則で定める基準に従い、当該保有個人情報を加工する。

2　前項の規定は、機構から独立行政法人等非識別加工情報の作成の委託を受けた者が受託した業務を行う場合について準用する。

(独立行政法人等非識別加工情報に関する事項の個人情報ファイル簿への記載)

第 36 条　機構は、独立行政法人等非識別加工情報を作成したときは、当該独立行政法人等非識別加工情報の作成に用いた保有個人情報を含む個人情報ファイルについては、個人情報ファイル簿に次に掲げる事項を記載する。

(1)　独立行政法人等非識別加工情報の概要として独立行政法人等非識別加工情報の本人の数及び独立行政法人等非識別加工情報に含まれる情報の項目

(2)　作成された独立行政法人等非識別加工情報の提案を受ける組織の名称及び所在地

(3)　作成された独立行政法人等非識別加工情報の提案をすることができる期間

(作成された独立行政法人等非識別加工情報をその用に供して行う事業に関する提案等)

第 37 条　前条の規定により個人情報ファイル簿に同条第 1 号に掲げる事項が記載された独立行政法人等非識別加工情報をその事業の用に供する独立行政法人等非識別加工情報取扱事業者になろうとする者は、機構に対し、当該事業に関する提案をすることができる。当該独立行政法人等非識別加工情報について第 34 条により独立行政法人等非識別加工情報の利用に関する契約を締結した者が、当該独立行政法人等非識別加工情報をその用に供する事業を変更しようとするときも、同様とする。

2　第 30 条第 2 項及び第 3 項、第 31 条、第 32 条並びに第 34 条は、前項の提案について準用する。

(手数料)

第 38 条　第 34 条(前条第 2 項において準用する場合を含む。次条において同じ。)の規定

により独立行政法人等非識別加工情報の利用に関する契約を締結する者は、機構の定めるところにより、手数料を納めなければならない。
2　前項の手数料の額は、実費を勘案し、かつ、行政法第 44 条の 13 の手数料の額を参酌して、機構が定める。
3　独立行政法人等は、前二項の規定による定めを一般の閲覧に供しなければならない。
(独立行政法人等非識別加工情報の利用に関する契約の解除)
第 39 条　機構は、第 34 条により独立行政法人等非識別加工情報の利用に関する契約を締結した者が次の各号のいずれかに該当するときは、当該契約を解除することができる。
(1)　偽りその他不正の手段により当該契約を締結したとき。
(2)　第 31 条各号(第 37 条第 2 項において準用する場合を含む。)のいずれかに該当することとなったとき。
(3)　当該契約において定められた事項について重大な違反があったとき。
(安全確保の措置)
第 40 条　機構は、独立行政法人等非識別加工情報等の漏えいを防止するために規則で定める基準に従い、次のとおり独立行政法人等非識別加工情報等の適切な管理のために必要な措置を講ずる。
(1)　独立行政法人等非識別加工情報等を取り扱う者の権限及び責任を明確に定める。
(2)　独立行政法人等非識別加工情報等の取扱いに関する規程類を整備し、当該規程類に従って独立行政法人等非識別加工情報等を適切に取り扱うとともに、その取扱いの状況について評価を行い、その結果に基づき改善を図るために必要な措置を講ずる。
(3)　独立行政法人等非識別加工情報等を取り扱う正当な権限を有しない者による独立行政法人等非識別加工情報等の取扱いを防止するために必要かつ適切な措置を講ずる。
2　前項の規定は、機構から独立行政法人等非識別加工情報等の取扱いの委託を受けた者が受託した業務を行う場合について準用する。
第 10 章　安全管理上の問題への対応
(事案の報告、再発防止措置及び公表等)
第 41 条　機構は、保有個人情報等の漏えい等安全管理の上で問題となる事案若しくは事案の恐れのある事実(以下「事案等」という。)が発生した場合又は発見された場合は、直ちに必要な措置を講ずるものとする。
2　役職員等及び情報取扱事務従事者は、事案等を直ちに課等責任者に報告しなければならない。
3　事案等の報告があった場合に課等責任者はその旨を責任者に報告し、責任者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずるものとする。
4　責任者は、事案等の報告があったときは、事案等発生の経緯、被害状況を調査し、統括責任者に報告する。統括責任者は、当該事案等が機構の個人情報安全管理等に重大な影響を及ぼすおそれがあると判断した場合は、最高責任者に報告しなければならない。

5　最高責任者は、前項の規定による報告を受けたときは当該事案等への対策案を委員会の議に付す。
6　最高責任者は、事案等の内容等に応じて、事案等の内容、経緯、被害状況等について、外務省に対して速やかに情報提供を行うこととする。
7　責任者は、事案等の発生した原因を分析し、再発防止のために必要な措置を講ずるものとする。
8　最高責任者は、事案等の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案等に係る本人への対応等の措置を講ずるものとする。なお、公表を行う事案等については、当該事案等の内容、経緯、被害状況等について、外務省と協議の上、速やかに必要な機関に対し情報提供を行う。

第 11 章　教育研修

(教育研修)

第 42 条　最高責任者は、保有個人情報等の取扱いに従事する役職員等及び情報事務従事者に対し、その保護に関する意識の高揚を図るための啓発その他必要な教育研修を定期的に行う。
2　最高責任者は、保有個人情報等を取り扱う情報システムの管理に関する事務に従事する役職員等及び情報事務従事者に対し、保有個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。
3　最高責任者は、責任者及び課等責任者に対し、現場における保有個人情報等の適切な管理のための教育研修を実施する。
4　責任者は、その所属する部等の役職員等及び情報取扱事務従事者に対し、保有個人情報等の適切な管理のために、最高責任者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずるものとする。

第 12 章　監査及び点検の実施

(点検)

第 43 条　責任者は、自ら管理責任を有する保有個人情報等の記録媒体、処理経路、保管方法等について、定期に又は随時に点検を行う。
2　責任者は、統括責任者に前項の点検結果を報告し、改善措置を提案する。
3　統括責任者は、前項に定める提案の内容に基づき、必要と判断する場合は、個人情報保護関連規程の改正の手続をとらなければならない。業務上重要な影響を及ぼすと認められるものについては、改正案を委員会の議に付さなければならない。

(監査)

第 44 条　監査責任者は、保有個人情報等の適切な管理を検証するため、機構における保有個人情報等の管理状況について、定期に及び必要に応じ随時に監査(外部監査を含む。)を行い、その結果を最高責任者に報告する。

(評価及び見直し)

第 45 条　保有個人情報等の適切な管理のための措置については､最高責任者､統括責任者、責任者等は、監査又は点検の結果を踏まえ、実効性の観点から保有個人情報等の適切な管理ための措置について評価し､必要があると認めるときは､その見直し等の措置を講ずる。

第 13 章　行政機関との連携

(行政機関との連携)

第 46 条　機構は、「個人情報の保護に関する基本方針」(平成 16 年 4 月 2 日閣議決定)4 を踏まえて、外務省と緊密に連携して、その保有個人情報等の適切な管理を行う。

第 14 章　雑則

(実施細目)

第 47 条　この細則の実施に必要な手続その他の細目(次項に規定する事項を除く。)は、情報システム室長が別に定める。

2　個人情報保護に係る開示、訂正及び利用停止、特定個人情報の取り扱い並びに独立行政法人非識別加工情報の提供に関する手続きその他の細目は、総務部長が別に定める。

附　則

この細則は、平成 17 年 4 月 1 日から施行する。

附　則(平成 20 年 4 月 1 日細則(総)第 5 号)

1　この細則は、平成 20 年 4 月 1 日から施行する。

2　この細則の施行に伴い、第 1 条から第 27 条までの規定により改正される各細則の規定により、当該各細則の実施に係る細目の決定を理事長から授権又は委任される者(以下「授権者」という。)が異なることとなる場合であって、この細則の施行の際、現に制定済の準内部規程等の細目(以下「準内部規程等」という。)があるときは、当該準内部規程等に相当する準内部規程等が新たな授権者により別途制定されるまでの間、現に制定済の準内部規程等を当該新たな授権者により制定されたものとみなす。

附　則(平成 20 年 11 月 14 日細則（情）第 51 号)

この細則は、平成 20 年 11 月 14 日から施行し、平成 20 年 10 月 1 日から適用する。

附　則(平成 21 年 3 月 16 日細則(情)第 8 号)

この細則は、平成 21 年 3 月 16 日から施行する。

附　則(平成 22 年 6 月 28 日細則(情)第 33 号)

この細則は、平成 22 年 6 月 28 日から施行する。
附　則(平成 23 年 3 月 31 日細則(情)第 9 号)

1　この細則は、平成 23 年 4 月 1 日から施行する。
2　この細則により、細則の実施に係る細目の決定を理事長から授権又は委任される者（以下「授権者」という。）が異なることとなる場合であって、この規程の施行の際、現に制定済の準内部規程等の細目（以下「準内部規程等」という。）があるときは、当該準内部規程等に相当する準内部規程等が新たな授権者により別途制定されるまでの間、現に制定済の準内部規程等を当該新たな授権者により制定されたものとみなす。
附　則(平成 23 年 12 月 12 日細則(情)第 49 号)

この細則は、平成 23 年 12 月 12 日から施行する。
附　則(平成 27 年 6 月 12 日細則(情)第 13 号)

この細則は、平成 27 年 6 月 12 日から施行する。
附　則(平成 27 年 9 月 30 日細則(情)第 20 号)

この細則は、平成 27 年 9 月 30 日から施行する。
附　則(平成 29 年 5 月 2 日細則(情)第 12 号)

1　この細則は、平成 29 年 5 月 30 日から施行する。
2　この細則により、細則の実施に係る細目の決定を理事長から授権又は委任される者（以下「授権者」という。）が異なることとなる場合であって、この細則の施行の際、現に制定済の準内部規程等の細目（以下「準内部規程等」という。）があるときは、当該準内部規程等に相当する準内部規程等が新たな授権者により別途制定されるまでの間、現に制定済の準内部規程等を当該新たな授権者により制定されたものとみなす。